D3.2
The HEIR 1st layer of services package: 1st complete version

Project number	883275
Project acronym	HEIR
Project title	A secure Healthcare Environment for Informatics Resilience
Start date of the project	September 1st, 2020
Duration	36 months
Programme	H2020-SU-DS-2019

Deliverable type	Demonstrator
Deliverable reference no.	D3.2
Workpackage	WP3
Due date	**28/02/2022 [M18]**
Actual submission date	18/03/2022

Deliverable lead	Bitdefender (BD)
Editors	Ovidiu Mihăilă
Contributors	Michalis Vakalellis (Aegis), Michalis Smyrlis (Sphynx), Andreas Zacharakis (STS), Gabriel Danciu (SIE), Bogdan Prelipcean (BD)
Reviewers	Eftychia Lakka (FORTH), Nikos Dimakopoulos (ITML)
Dissemination level	PU
Revision	1.0
Keywords	#servicespackage #heirarchitecture #heirframework #cybersecurity

Abstract

Deliverable 3.2 serves as the document illustrating the achieved progress of implementing the complete version of HEIR's 1st layer of services package. The work reflected within this report has been conducted between M13 and M18 and involved the partners' personnel active within WP3 and the connecting WPs such as WP2, WP4 and WP5.

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275

Executive Summary

The current deliverable presents the work that has been carried out towards the delivery of the HEIR's 1st layer of services package – the 1st complete version. The development from the initial MVP version demonstrates the effective implementation of the 1st layer components within a consistent integrated framework that showcases the impact of the proposed solution.

The 1st layer of services package for this intermediate version includes: (I) the novel HEIR Client; (II) the Threat Detection Module and the services for the RAMA score calculations at different levels; (III) the toolset for the visualisation of the HEIR reported security levels, incidents, threats, statistics, etc. and (IV) the novel HEIR Aggregators.

The demonstrator will be presented in a short report. This intermediate version of the 1st layer of services package serves as an advancement since the MVP version (M12) and the foundation which will drive the implementation toward the release of final version (M30).

Table of Contents

List of Figures

1. Introduction

1.1 Scope and objectives

HEIR Project aims to provide healthcare units with tools and services for threat identification and cybersecurity knowledge base system. HEIR comprises four “use-cases” – two healthcare units from Greece, one from United Kingdom and one from Norway. The variations within technical infrastructures size, complexity and personnel, the geographic localisation together with the different regulations were considering when the HEIR architecture was initiated, designed and developed. Starting from these assumptions, the report provides the overview of the advancements, starting from the work reported in deliverable D3.1 – The HEIR 1st layer of services package for the MVP.

1.2 Relation to other Tasks and Work Packages

The current deliverable is part of ***WP3 – HEIR client and aggregator*** and continues the presentation initiated by D3.1. It is regarded as an intermediate snapshot of the current status of HEIR’s 1st layer of services, between the MVP (M12) and the final version (M26). The document reflects the activities done from T3.1 to T3.4 as well as the connections with WP2, WP4 and WP5 activities:

- “D4.2 - The HEIR 2nd layer of services package: 1st complete version”, as the 2nd layer contains the HEIR global benchmark against which the RAMA scores of medical infrastructures will be compared.
- “D5.3 – HEIR integrated framework intermediate version” as HEIR 1st layer of services packaging will be part of the overall HEIR framework.

1.3 Structure of the document

The remainder of the document walks the reader through the three sections. Firstly, the complete version of the HEIR’s 1st layer of services is described, followed by the PAGNI deployment and finalising with the conclusions. These presentation sections are complemented by three technical Annexes whose scope is to showcase the samples output.

2. The HEIR 1st layer of services.

2.1 Overview

This subsection presents an overview of architecture for the 1st layer of services package. The figure below illustrates a high-level overview of the architecture and its various components within the 1st layer. More specifically, the components are:

- the HEIR Client,
- the local RAMA Score Calculator
- the HEIR Client Graphical Unit
- the HEIR Aggregator.

2.2 The HEIR Client

The HEIR Client is the central component that collects and centralize data received from the facilitators and from the HEIR Client Components. The HEIR Client role is depicted in Figure 1.

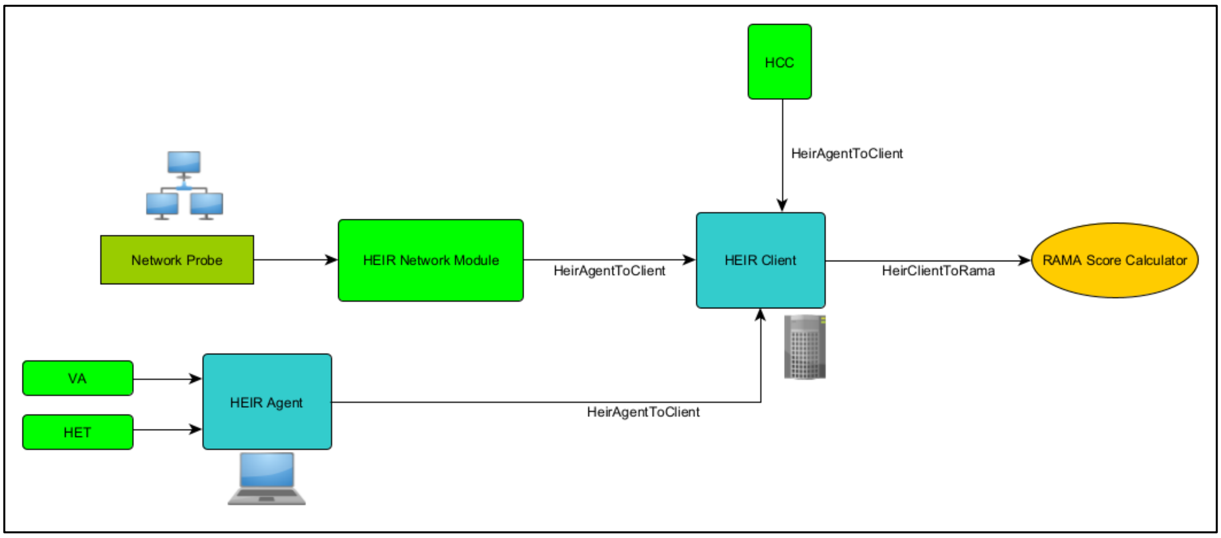


Figure 1. HEIR Client overview

From the MVP to the 1st complete version the HEIR Client was separated from the HeirAgent and deployed as a separate component. It is implemented in Python and deployed as dockerised component. Besides the existing components that were available in the MVP and remained integrated with the HeirAgent, the HEIR Client also accommodate the data from the new implemented component: HEIR Network Module and HEIR Cryptographic Checker.

The communications are made through the Kafka message broker. The data received from the facilitators (in this case HeirAgent) the HEIR Components are submitted on HeirAgentToClient topic and then consumed by the HEIR Client.

The HEIRClient assures that the received schema from the input module is correct, aggregates the data for the same client id (the client id has a corresponding department of interest associated) and the submits the centralized data further to the RAMA Score Calculator on the existing HeirClientToRama topic.

2.2.1 The HEIR Network Module

The HEIR Network Module is having the role to monitor the network traffic and provide security insight regarding malicious activity. For the 1st complete version of 1st layer of services package, the HEIR Network Module (HNM) can analyse the inbound and outbound network traffic with the following outcome.

- The HNM can detect:
  - Private information leaks
  - Malicious content sent over the network (threat detection ability)
  - On-going attacks over the network
- The HNM can provide:
  - Connection information for the endpoints connected to the analysed network
  - Usage statistics that can be used for anomaly detection.

The HNM has the following internal components:

- Network probe – that intercepts the traffic for the ethernet device and (sub)network that is configured.
- Detection component – that analyse the extracted traffic. It contains threat detection signatures and heuristic rules, measures the indicators for attack. It also has patterns for information leaks over the network.
- HNM producer – this component collects the data from the detection components, process it and then submits the output to the HeirClient through the message broker.

The HNM is based on and improves the Bitdefender's technologies regarding network traffic analysis for the healthcare environments.

2.2.2 The HEIR Exploit Tester

The HEIR Exploit Tester (HET) has the role to assess the attack surfaces for the operating system configuration. In this moment the HEIR Exploit Tester has the same functionality from the MVP but contains an updated set of rules to detect misconfigurations and vulnerabilities from the operating system.
As an input it queries the registry keys, configuration parameters from the Windows Operating system and the output are the list of the misconfigured items regarding security concerns with recommendations and descriptions.

2.2.3 The HEIR Cryptographic Checker

The HEIR Cryptographic Checker (HCC) has the role to alert regarding the usage of outdated security protocol that are used inside the HEIR environment servers or to target the outside servers that are service providers for the HEIR system inside the environments.
The HCC tools are based on the open-source tool SSLScan[1] and it can detect

- The used protocol and version. This can be cross listed with the required one (latest version is recommended as default.
- Usage of vulnerable cryptographic implementations.

The output of HCC is submitted to the HEIR Client.

2.3 The Local RAMA Score Calculator

The MVP version of the local RAMA Score calculator, reported in "D3.1 – The HEIR 1st layer of services package for the MVP" received input from the HEIR Exploit Tester and Vulnerability assessment. During the 1st complete version of the local RAMA, major updates occurred contributed to a score that better depicts the organisations attack surface. More specifically, the 1st complete version of the local RAMA Score calculator incorporates all the

[1] GitHub - rbsec/sslscan: sslscan tests SSL/TLS enabled services to discover supported cipher suites

different modules of the HEIR client, namely, (a) the HEIR Exploit Tester (HET) , (b) the Vulnerability assessment (VA), (c) the HEIR Network Module (HNM) , and (d) the HEIR Cryptographic Checker (HCC). This allows the RAMA Score calculator to consider issues identified in different layers of a computing system, e.g., network, presentation and application layer, and, subsequently, provides a score (and the corresponding metadata) that would allow the end user to have a better understanding of the security posture of its organisation. Moreover, the local RAMA Score is now calculated based on the creation of two different sub-scores. The first sub-score, namely, the base score, is an aggregation of the HET, HCC and VA sub-scores. The rationale behind this, is that the tools will not be continually triggered by the HEIR client, as they are used for the "static" analysis part of a computing system. On the other hand, the second sub-score, namely, the temporal score, is based on the HNM component. Since attacks on the network layer are more frequent, the temporal score will also be calculated in a more frequent way than the base one. That being said, the final, aggregated Local RAMA Score is a weighted sum of the two sub scores as depicted in the equation below.

$$Local\ RAMA\ Score = 70\% * Base\ score + 30\% * Temporal\ Score$$

The local Rama Score also creates the security exposure of an organisation, as follows:

- 100 = None
- 80 – 99 = Low
- 50 – 79 = Medium
- 10 – 49 = High
- 0 – 9 = Critical

2.3.1 Local RAMA sub-scores

2.3.1.1.1 Base Score

As mentioned, the base score is a weighted sum (average) of the HET, HCC and VA sub-scores. More specifically, the weighted sum is defined as

$$Base\ Score = \sum_{i=1}^{3} \frac{(x_i - \min(x))}{(\max(x) - \min(x))} * 100$$

Where xi is the aforementioned sub-scores, min(x) = 0 and max(x) = 300.

2.3.1.1.1.1 HEIR Exploit Tester sub-score and metadata

HEIR Exploit tester (see Section 2.2.2) reports vulnerabilities and misconfigurations identified within a system. To that end, the HET sub-score is a weighted average between these two issues as depicted below.

$$HET\ score = 0.85 * vulnerability\_score\ + 0.25 * misconfiguration\_score$$

The formula for the calculation of the vulnerability and misconfiguration score takes into consideration (a) the impact per identified security property, i.e., confidentiality, integrity, and availability, and (b) the triggered value. More specifically, if a specific vulnerability/misconfiguration was triggered, then the weight is being added as below.

$$Vulnerability_{score} = \sum_{i=1}^{n} CISi + IISi + AISi$$

$$Misconfiguration_{score} = \sum_{i=1}^{n} CISi + IISi + AISi$$

where n is the total number of vulnerabilities/misconfigurations, CISi is the Confidentiality Impact Score, IISi is the integrity impact score and AISi is the Availability impact score.

The score per impact is calculated based on the impact value, as depicted below.

Impact value:

- None = 0
- Low = 2
- Medium = 7
- High = 10

Finally, the vulnerability and misconfiguration score, and the final HET score is normalised from 0 – 100.

Lastly, the metadata created by the Local RAMA Score calculator regarding the HET include: (a) the number and percentage of malicious findings, (b) the number of operating system vulnerabilities, (c) the number of misconfigurations, (d) the number and percentage of benign findings, and (e) the HET vector, a vector that shows the qualitative impact per security property (CIA).

2.3.1.1.1.2 *Vulnerability Assessment Score*

The vulnerability assessment identifies vulnerabilities per deployed application (unlike the HET which identified them in the operating system).

The formula for the calculation of the vulnerability assessment score takes into consideration (a) the number of identified applications, and (b) the identified vulnerabilities per application, as shown in the formula below.

$$VA = \sum_{i=1}^{n} Ai * Vs$$

where n is the total number of applications, Ai is the applications and Vs is the vulnerability score per application.

The vulnerability score (Vs) takes into consideration the severity per vulnerability (as provided by the VA), as depicted below.

$$Vs = \sum_{i=1}^{n} VSSi$$

Where n is the total number of vulnerabilities and VSSi is the vulnerability severity score based on the severity.

The severity per vulnerability is calculated as follow.

Severity value:

- 0-20 = 1
- 21-50 = 3
- 51-80 = 5
- 81-100 = 7

Finally, both the vulnerability assessment, and the vulnerability score is normalised from 0 – 100.

Lastly, the metadata created by the Local RAMA Score calculator regarding the VA include: (a) the total number of identified vulnerabilities per application and their CVE Id, (b) the total number of vulnerabilities (for all applications), and (c) the top 10 vulnerabilities.

2.3.1.1.1.3 *HEIR Cryptographic Checker (HCC) score*

The HEIR Cryptographic checker identifies issues related to the cryptographic protocols used within a system.

The formula for the calculation of the HCC score takes into consideration the heart bleeds reported by the HCC. If, a specific TLS version, is being enabled (enabled = 1 in the protocols) and is vulnerable (vulnerable =1), then the HCC score is increased by 10 (as it is considered a major issue). The formula is depicted below.

$$HCC_{score} = \sum_{i=1}^{n} Hi$$

where n is the total number of identified heart bleeds and Hi=10.
Finally, the HCC score is normalised from 0 – 100.
Lastly, the metadata created by the Local RAMA Score calculator regarding the HCC include: (a) the list of identified vulnerable TLS protocols and (b) the number of these protocols.

2.3.1.1.2 Temporal score

The temporal score, for the 1st complete version of the Local RAMA, will be equal to the HNM score.

2.3.1.1.2.1 HNM Score

The HEIR Network Module is responsible to identify issues in the network layer.
The formula for the calculation of the HNM score takes into consideration the alert type reported by the HNM as this reveals the severity of the identified issue. More specifically, the alert type could be (a) none, (b) info, (c) suspicious, (d) malware, (e) attack, and (f) exploit. Based on this, the HNM formula is as follows.

$$HNM_{score} = \sum_{i=1}^{n} NISi$$

where n is the total number of identified network issues (alerts or detections) and NISi is the network impact score.
NIS is calculated as:

- None = 0
- Info = 2
- Suspicious = 4
- Malware = 6
- Attack = 8
- Exploit = 10

Finally, the HNM score is normalised from 0 – 100.
Lastly, the metadata created by the Local RAMA Score calculator regarding the HNM include: (a) the number of exploits, (b) the number of attacks, (c) the total number of findings and (d) the destination port and IP, the source port and IP and a brief description per network issue.

2.3.2 Local RAMA Score calculator deployment information

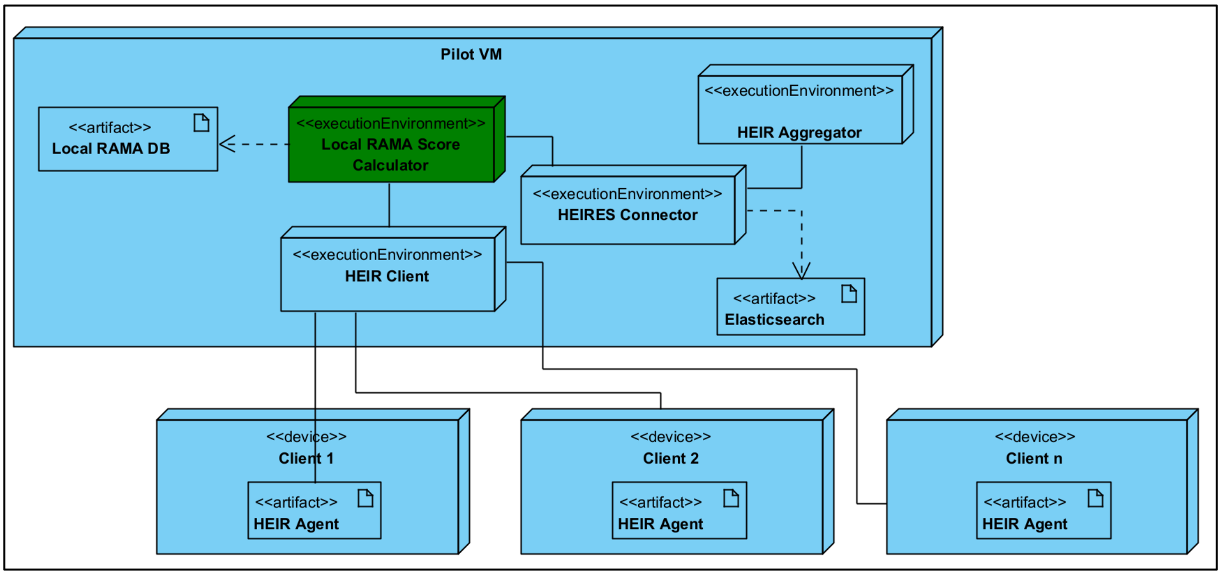


Figure 2. Local RAMA Score calculation deployment diagram

As depicted in *Figure 2*, the local RAMA Score calculator is deployed inside the HEIR pilot's VM. It communicates with the HEIR client (receives data) and the HEIRES Connector (provides output). Moreover, the local RAMA Score calculator stores the data in the Local RAMA DB.

Lastly, the local RAMA scores (and sub-scores) and the metadata, are being visualised through the HEIR Client GUI (see Section 2.4).

A sample output of the 1st complete RAMA Score is available in Appendix A – 1st complete version of the HEIR Client sample output

```
{
    "clientId": 1234,
    "connected_clients": 1,
    "het": [
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Verifies the local group policy settings for
User Configuration\\Administrative Templates\\System\\Ctrl+Alt+Del
Options\\Remove Task Manager. When Remove Task Manager is enabled, the
endpoint is vulnerable to security threats. Since Task Manager can list and
terminate currently running processes, some malware may disable it to
prevent themselves from being closed.",
            "integrity": "None",
            "name": "Task Manager",
            "score": 25,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Verifies if Windows requires account sign-in.
When the user accounts sign-in is disabled, Windows stores the user
passwords in the registry database, making possible to bypass the password
screen during logon.",
            "integrity": "None",
            "name": "Auto Logon",
            "score": 25,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Low",
            "description": "Verifies the local security policy option User
Account Control: Run all administrators in Admin Approval Mode. This
setting controls the behavior of all UAC policy settings for the endpoint.
UAC (User Account Control) is a security feature that helps preventing
unauthorized changes to the OS by potentially harmful programs. UAC
requires administrator authorization for actions like installing a program
or modifying system settings. When UAC is set to Never notify, the system
is more vulnerable to malware.",
            "integrity": "Low",
            "name": "UAC Off",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Low",
            "description": "Verifies the configuration for User Account
Control policy and registry settings, to check if these comply with the
default recommended settings. The policy settings are located in Security
Settings\\Local Policies\\Security Options, in the Local Security Policy
app.",
            "integrity": "Low",
            "name": "UAC Insecure",
            "score": 30,
            "triggered": true,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Verifies the local group policy Turn off Data
Execution Prevention for Explorer, located in Computer
Configuration\\Administrative Templates\\Windows Components\\File Explorer.
Disabling data execution prevention can allow certain legacy plug-in
applications to function without terminating Explorer.",
            "integrity": "Low",
            "name": "Explorer Data Execution Prevention",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Verifies the local group policy Turn off heap
termination on corruption, located in Computer
Configuration\\Administrative Templates\\Windows Components\\File Explorer.
Disabling heap termination on corruption can allow certain legacy plug-in
applications to function without terminating Explorer immediately, although
Explorer may still terminate unexpectedly later.",
            "integrity": "Low",
            "name": "Heap Termination on Corruption",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Verifies the local group policy Do not allow 
passwords to be saved, located in Computer Configuration\\Administrative 
Templates\\Windows Components\\Remote Desktop Services\\Remote Desktop 
Connection Client. This policy controls whether passwords can be saved on 
this computer from Remote Desktop Connection.  - If you enable this 
setting, the password saving checkbox in Remote Desktop Connection will be 
disabled and users will no longer be able to save passwords. When a user 
opens an RDP file using Remote Desktop Connection and saves his settings, 
any password that previously existed in the RDP file will be deleted.",
            "integrity": "Low",
            "name": "Save Passwords from RDP",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Verifies the local group policy Do not allow 
drive redirection, located in Computer Configuration\\Administrative 
Templates\\Windows Components\\Remote Desktop Services\\Remote Desktop 
Session Host\\Device and Resource Redirection. This policy setting 
specifies whether to prevent the mapping of client drives in a Remote 
Desktop Services session (drive redirection). By default, an RD Session 
Host server maps client drives automatically upon connection. Mapped drives 
appear in the session folder tree in File Explorer or Computer in the 
format &lt;driveletter&gt; on &lt;computername&gt;. You can use this policy 
setting to override this behavior.  - If you enable this policy setting, 
client drive redirection is not allowed in Remote Desktop Services 
sessions, and Clipboard file copy redirection is not allowed on computers 
running Windows Server 2003, Windows 8, and Windows XP.",
            "integrity": "Low",
            "name": "Drive Redirection",
            "score": 50,
            "triggered": true,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Checks the Macro settings for Office Word 16, 
located in File\\Options\\Trust Center\\Trust Center Settings\\Macro 
Settings. Disable all macros without notification - Macros and security 
alerts about macros are disabled. Disable all macros with notification - 
Macros are disabled, but security alerts will be triggered if macros are 
present. Disable all macros except digitally signed macros - Macros are 
disabled, but security alerts will be triggered if macros are present. 
However, for macros digitally signed by a trusted publisher, these will run 
if the trust access for that publisher has been enabled. Enable all macros 
(not recommended, potentially dangerous code can run) - All macros run. 
This setting makes your computer vulnerable to potentially malicious code. 
Trust access to the VBA project object model.",
            "integrity": "Medium",
            "name": "Office Word 16 Macro",
            "score": 55,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Checks the Macro settings for Office Excel 16, 
located in File\\Options\\Trust Center\\Trust Center Settings\\Macro 
Settings. Disable all macros without notification - Macros and security 
alerts about macros are disabled. Disable all macros with notification - 
Macros are disabled, but security alerts will be triggered if macros are 
present. Disable all macros except digitally signed macros - Macros are 
disabled, but security alerts will be triggered if macros are present. 
However, for macros digitally signed by a trusted publisher, these will run 
if the trust access for that publisher has been enabled. Enable all macros 
(not recommended, potentially dangerous code can run) - All macros run. 
This setting makes your computer vulnerable to potentially malicious code. 
Trust access to the VBA project object model.",
            "integrity": "Medium",
            "name": "Office Excel 16 Macro",
            "score": 55,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Checks the Macro settings for Office Outlook 
16, located in File\\Options\\Trust Center\\Trust Center Settings\\Macro 
Settings. Disable all macros without notification - Macros and security 
alerts about macros are disabled. Disable all macros with notification - 
Macros are disabled, but security alerts will be triggered if macros are 
present. Disable all macros except digitally signed macros - Macros are 
disabled, but security alerts will be triggered if macros are present. 
However, for macros digitally signed by a trusted publisher, these will run 
if the trust access for that publisher has been enabled. Enable all macros 
(not recommended, potentially dangerous code can run) - All macros run. 
This setting makes your computer vulnerable to potentially malicious code. 
Trust access to the VBA project object model.",
            "integrity": "Medium",
            "name": "Office Outlook 16 Macro",
            "score": 55,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Low",
            "description": "Checks the number of local administrators on 
the machine.",
            "integrity": "None",
            "name": "Too many local administrators",
            "score": 40,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "High",
            "description": "Checks the existence of shared folders with 
read access for the Everyone group. The Everyone group includes all users 
who have logged in with a password (members of the Authenticated Users 
group) as well as built-in, non-password protected accounts such as Guest,
and several other built-in security accounts like SERVICE, LOCAL_SERVICE,
NETWORK_SERVICE, and others. A Guest account is a built-in account on a
Windows system that is disabled by default.  - If enabled, it allows anyone
to login without a password.",
            "integrity": "None",
            "name": "SMB Shared Everyone Read",
            "score": 20,
            "triggered": true,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Checks the existence of shared folders with
write access for the Everyone group. The Everyone group includes all users
who have logged in with a password (members of the Authenticated Users
group) as well as built-in, non-password protected accounts such as Guest,
and several other built-in security accounts like SERVICE, LOCAL_SERVICE,
NETWORK_SERVICE, and others. A Guest account is a built-in account on a
Windows system that is disabled by default.  - If enabled, it allows anyone
to login without a password.",
            "integrity": "Medium",
            "name": "SMB Shared Everyone Write",
            "score": 25,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "High",
            "description": "Verifies if regular users are allowed to read
the Security Account Manager (SAM) data. Non-admin users should not be
allowed to read critical files, but a vulnerability (known as HiveNightmare
or SeriousSam) has been discovered in Windows 11 and Windows 10 version
1809 and above, which involved a \"bad\" ACL being set on the
%SystemRoot%\\System32\\Config folder, making it possible for regular users
to acces the SAM, SYSTEM, SECURITY and other critical files.",
            "integrity": "Medium",
            "name": "SAM File readable by users",
            "score": 80,
            "triggered": false,
            "type": "Vulnerability"
        }
    ],
    "hospitalId": 5678,
    "hospital_address": "Street no 1",
    "hospital_region": "Hospital A from region B",
    "host_name": "HOST-L2",
    "host_os": "Windows 10",
    "machine_id":
"3119BFD93119E3AB3119D0123119960B3119B2ED3119FDE63119DF543119C5BB3119FC3531
1994B33119DB3C3119D9C23119A1363119BCC73119BDB63119F25A",
    "scan_id": "00943c780094363d00940dfd00944745",
    "scan_status": "finished",
    "vulnerabilityAssessment": [
        {
            "application_name": "Mozilla Firefox",
            "cves": [
                {
                    "cve": "CVE-2007-3670",
                    "description": "Argument injection vulnerability in
Microsoft Internet Explorer, when running on systems with Firefox installed
and certain URIs registered, allows remote attackers to conduct cross-
browser scripting attacks and execute arbitrary commands via shell
metacharacters in a (1) FirefoxURL or (2) FirefoxHTML URI, which are
inserted into the command line that is created when invoking firefox.exe.
NOTE: it has been debated as to whether the issue is in Internet Explorer
or Firefox. As of 20070711, it is CVE's opinion that IE appears to be
failing to properly delimit the URL argument when invoking Firefox, and
this issue could arise with other protocol handlers in IE as well. However,
Mozilla has stated that it will address the issue with a
\\\\\\\\\\\\\\\"defense in depth\\\\\\\\\\\\\\\" fix that will
\\\\\\\\\\\\\\\"prevent IE from sending Firefox malicious
data.\\\\\\\\\\\\\\\"",
                    "publish_date": "2007-07-10T19:30Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2011-0064",
                    "description": "The hb_buffer_ensure function in hb-
buffer.c in HarfBuzz, as used in Pango 1.28.3, Firefox, and other products,
does not verify that memory reallocations succeed, which allows remote
attackers to cause a denial of service (NULL pointer dereference and
application crash) or possibly execute arbitrary code via crafted OpenType
font data that triggers use of an incorrect index.",
                    "publish_date": "2011-03-07T21:00Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2011-3389",
                    "description": "The SSL protocol, as used in certain
configurations in Microsoft Windows and Microsoft Internet Explorer,
Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by
using CBC mode with chained initialization vectors, which allows man-in-
the-middle attackers to obtain plaintext HTTP headers via a blockwise
chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with
JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java
URLConnection API, or (3) the Silverlight WebClient API, aka a
\\\\\\\\\\\\\\\"BEAST\\\\\\\\\\\\\\\" attack.",
                    "publish_date": "2011-09-06T19:55Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2015-4000",
                    "description": "The TLS protocol 1.2 and earlier, when
a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does
not properly convey a DHE_EXPORT choice, which allows man-in-the-middle
attackers to conduct cipher-downgrade attacks by rewriting a ClientHello
with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with
DHE_EXPORT replaced by DHE, aka the \\\\\\\\\\\\\\\"Logjam\\\\\\\\\\\\\\\"
issue.",
                    "publish_date": "2015-05-21T00:59Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23987",
                    "description": "Mozilla developers and community
members reported memory safety bugs present in Firefox 86 and Firefox ESR
78.8. Some of these bugs showed evidence of memory corruption and we
presume that with enough effort some of these could have been exploited to
```

```
run arbitrary code. This vulnerability affects Firefox ESR < 78.9, Firefox
< 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23988",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 86. Some of these bugs showed evidence of
memory corruption and we presume that with enough effort some of these
could have been exploited to run arbitrary code. This vulnerability affects
Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23984",
                    "description": "A malicious extension could have opened
a popup window lacking an address bar. The title of the popup lacking an
address bar should not be fully controllable, but in this situation was.
This could have been used to spoof a website and attempt to trick the user
into providing credentials. This vulnerability affects Firefox ESR < 78.9,
Firefox < 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23986",
                    "description": "A malicious extension with the 'search'
permission could have installed a new search engine whose favicon
referenced a cross-origin URL. The response to this cross-origin request
could have been read by the extension, allowing a same-origin policy bypass
by the extension, which should not have cross-origin permissions. This
cross-origin request was made without cookies, so the sensitive information
disclosed by the violation was limited to local-network resources or
resources that perform IP-based authentication. This vulnerability affects
Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23981",
                    "description": "A texture upload of a Pixel Buffer
Object could have confused the WebGL code to skip binding the buffer used
to unpack it, resulting in memory corruption and a potentially exploitable
information leak or crash. This vulnerability affects Firefox ESR < 78.9,
Firefox < 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-23982",
                    "description": "Using techniques that built on the
slipstream research, a malicious webpage could have scanned both an
internal network's hosts as well as services running on the user's local
machine utilizing WebRTC connections. This vulnerability affects Firefox
ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23983",
                    "description": "By causing a transition on a parent
node by removing a CSS rule, an invalid property for a marker could have
been applied, resulting in memory corruption and a potentially exploitable
crash. This vulnerability affects Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23985",
                    "description": "If an attacker is able to alter
specific about:config values (for example malware running on the user's
computer), the Devtools remote debugging feature could have been enabled in
a way that was unnoticable to the user. This would have allowed a remote
attacker (able to make a direct network connection to the victim) to
monitor the user's browsing activity and (plaintext) network traffic. This
was addressed by providing a visual cue when Devtools has an open network
socket. This vulnerability affects Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29968",
                    "description": "When drawing text onto a canvas with
WebRender disabled, an out of bounds read could occur. *This bug only
affects Firefox on Windows. Other operating systems are unaffected.*. This
vulnerability affects Firefox < 89.0.1.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-29967",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 88 and Firefox ESR 78.11. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR <
78.11.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29966",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 88. Some of these bugs showed evidence of
memory corruption and we presume that with enough effort some of these
could have been exploited to run arbitrary code. This vulnerability affects
Firefox < 89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29947",
                    "description": "Mozilla developers and community
members reported memory safety bugs present in Firefox 87. Some of these
bugs showed evidence of memory corruption and we presume that with enough
effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29946",
                    "description": "Ports that were written as an integer
overflow above the bounds of a 16-bit integer could have bypassed port
blocking restrictions when used in the Alt-Svc header. This vulnerability
affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29964",
                    "description": "A locally-installed hostile program
could send `WM_COPYDATA` messages that Firefox would process incorrectly,
leading to an out-of-bounds read. *This bug only affects Firefox on
Windows. Other operating systems are unaffected.*. This vulnerability
affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-29961",
                    "description": "When styling and rendering an oversized
`<select>` element, Firefox did not apply correct clipping which allowed an
attacker to paint over the user interface. This vulnerability affects
Firefox < 89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29960",
                    "description": "Firefox used to cache the last filename
used for printing a file. When generating a filename for printing, Firefox
usually suggests the web page title. The caching and suggestion techniques
combined may have lead to the title of a website visited during private
browsing mode being stored on disk. This vulnerability affects Firefox <
89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29959",
                    "description": "When a user has already allowed a
website to access microphone and camera, disabling camera sharing would not
fully prevent the website from re-enabling it without an additional prompt.
This was only possible if the website kept recording with the microphone
until re-enabling the camera. This vulnerability affects Firefox < 89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29955",
                    "description": "A transient execution vulnerability,
named Floating Point Value Injection (FPVI) allowed an attacker to leak
arbitrary memory addresses and may have also enabled JIT type confusion
attacks. (A related vulnerability, Speculative Code Store Bypass (SCSB),
did not affect Firefox.). This vulnerability affects Firefox ESR < 78.9 and
Firefox < 87.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 26
                },
                {
                    "cve": "CVE-2021-29951",
                    "description": "The Mozilla Maintenance Service granted 
SERVICE_START access to BUILTIN|Users which, in a domain network, grants 
normal remote users access to start or stop the service. This could be used 
to prevent the browser update service from operating (if an attacker 
spammed the 'Stop' command); but also exposed attack surface in the 
maintenance service. *Note: This issue only affected Windows operating 
systems older than Win 10 build 1709. Other operating systems are 
unaffected.*. This vulnerability affects Thunderbird < 78.10.1, Firefox < 
87, and Firefox ESR < 78.10.1.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 64
                },
                {
                    "cve": "CVE-2021-29944",
                    "description": "Lack of escaping allowed HTML injection 
when a webpage was viewed in Reader View. While a Content Security Policy 
prevents direct code execution, HTML injection is still possible. *Note: 
This issue only affected Firefox for Android. Other operating systems are 
unaffected.*. This vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-24002",
                    "description": "When a user clicked on an FTP URL 
containing encoded newline characters (%0A and %0D), the newlines would 
have been interpreted as such and allowed arbitrary commands to be sent to 
the FTP server. This vulnerability affects Firefox ESR < 78.10, Thunderbird 
< 78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-24001",
                    "description": "A compromised content process could 
have performed session history manipulations it should not have been able 
to due to testing infrastructure that was not restricted to testing-only 
configurations. This vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-24000",
                    "description": "A race condition with 
requestPointerLock() and setTimeout() could have resulted in a user 
interacting with one tab when they believed they were on a separate tab. In 
conjunction with certain elements (such as &lt;input 
type=\\\\\\\\\\\\\\\"file\\\\\\\\\\\\\\\"&gt;) this could have led to an 
attack where a user was confused about the origin of the webpage and 
potentially disclosed information they did not intend to. This 
vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 26
                },
                {
                    "cve": "CVE-2021-23999",
                    "description": "If a Blob URL was loaded through some 
unusual user interaction, it could have been loaded by the System Principal 
and granted additional privileges that should not be granted to web 
```

```
content. This vulnerability affects Firefox ESR < 78.10, Thunderbird <
78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23998",
                    "description": "Through complicated navigations with
new windows, an HTTP page could have inherited a secure lock icon from an
HTTPS page. This vulnerability affects Firefox ESR < 78.10, Thunderbird <
78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23996",
                    "description": "By utilizing 3D CSS in conjunction with
Javascript, content could have been rendered outside the webpage's
viewport, resulting in a spoofing attack that could have been used for
phishing or other attacks on a user. This vulnerability affects Firefox <
88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23997",
                    "description": "Due to unexpected data type
conversions, a use-after-free could have occurred when interacting with the
font cache. We presume that with enough effort this could have been
exploited to run arbitrary code. This vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23995",
                    "description": "When Responsive Design Mode was
enabled, it used references to objects that were previously freed. We
presume that with enough effort this could have been exploited to run
arbitrary code. This vulnerability affects Firefox ESR < 78.10, Thunderbird
< 78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 50
                },
                {
                    "cve": "CVE-2021-23994",
                    "description": "A WebGL framebuffer was not initialized
early enough, resulting in memory corruption and an out of bound write.
This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and
Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29989",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox
< 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29988",
                    "description": "Firefox incorrectly treated an inline
list-item element as a block element, resulting in an out of bounds read or
memory corruption, and a potentially exploitable crash. This vulnerability
affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and
Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29987",
                    "description": "After requesting multiple permissions,
and closing the first permission panel, subsequent permission panels will
be displayed in a different position but still record a click in the
default location, making it possible to trick a user into accepting a
permission they did not want to. *This bug only affects Firefox on Linux.
Other operating systems are unaffected.*. This vulnerability affects
Firefox < 91 and Thunderbird < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29986",
                    "description": "A suspected race condition when calling
getaddrinfo led to memory corruption and a potentially exploitable crash.
*Note: This issue only affected Linux operating systems. Other operating
systems are unaffected.* This vulnerability affects Thunderbird < 78.13,
Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29985",
                    "description": "A use-after-free vulnerability in media
channels could have led to memory corruption and a potentially exploitable
crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91,
Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29984",
                    "description": "Instruction reordering resulted in a
sequence of instructions that would cause an object to be incorrectly
considered during garbage collection. This led to memory corruption and a
potentially exploitable crash. This vulnerability affects Thunderbird <
78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29983",
                    "description": "Firefox for Android could get stuck in
fullscreen mode and not exit it even after normal interactions that should
cause it to exit. *Note: This issue only affected Firefox for Android.
Other operating systems are unaffected.*. This vulnerability affects
Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29982",
                    "description": "Due to incorrect JIT optimization, we
incorrectly interpreted data from the wrong type of object, resulting in
the potential leak of a single bit of memory. This vulnerability affects
Firefox < 91 and Thunderbird < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29981",
                    "description": "An issue present in lowering/register
allocation could have led to obscure but deterministic register confusion
failures in JITted code that would lead to a potentially exploitable crash.
This vulnerability affects Firefox < 91 and Thunderbird < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29980",
                    "description": "Uninitialized memory in a canvas object
could have caused an incorrect free() leading to memory corruption and a
potentially exploitable crash. This vulnerability affects Thunderbird <
78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29990",
                    "description": "Mozilla developers and community
members reported memory safety bugs present in Firefox 90. Some of these
bugs showed evidence of memory corruption and we presume that with enough
effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38501",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR <
91.2.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38500",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR
< 91.2, Firefox ESR < 78.15, and Firefox < 93.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38499",
                    "description": "Mozilla developers reported memory 
safety bugs present in Firefox 92. Some of these bugs showed evidence of 
memory corruption and we presume that with enough effort some of these 
could have been exploited to run arbitrary code. This vulnerability affects 
Firefox < 93.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38498",
                    "description": "During process shutdown, a document 
could have caused a use-after-free of a languages service object, leading 
to memory corruption and a potentially exploitable crash. This 
vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 
91.2.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 50
                },
                {
                    "cve": "CVE-2021-38497",
                    "description": "Through use of reportValidity() and 
window.open(), a plain-text validation message could have been overlaid on 
another origin, leading to possible user confusion and spoofing attacks. 
This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox 
ESR < 91.2.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-38494",
                    "description": "Mozilla developers reported memory 
safety bugs present in Firefox 91. Some of these bugs showed evidence of 
memory corruption and we presume that with enough effort some of these 
could have been exploited to run arbitrary code. This vulnerability affects 
Firefox < 92.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38493",
                    "description": "Mozilla developers reported memory 
safety bugs present in Firefox 91 and Firefox ESR 78.13. Some of these bugs 
showed evidence of memory corruption and we presume that with enough effort 
some of these could have been exploited to run arbitrary code. This 
vulnerability affects Firefox ESR < 78.14, Thunderbird < 78.14, and Firefox 
< 92.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38492",
                    "description": "When delegating navigations to the 
operating system, Firefox would accept the `mk` scheme which might allow 
attackers to launch pages and execute scripts in Internet Explorer in 
unprivileged mode. *This bug only affects Firefox for Windows. Other 
operating systems are unaffected.*. This vulnerability affects Firefox < 
92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and 
Firefox ESR < 91.1.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-38491",
                    "description": "Mixed-content checks were unable to
analyze opaque origins which led to some mixed content being loaded. This
vulnerability affects Firefox < 92.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29991",
                    "description": "Firefox incorrectly accepted a newline
in a HTTP/3 header, interpretting it as two separate headers. This allowed
for a header splitting attack against servers using HTTP/3. This
vulnerability affects Firefox < 91.0.1 and Thunderbird < 91.0.1.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-38496",
                    "description": "During operations on MessageTasks, a
task may have been removed while it was still scheduled, resulting in
memory corruption and a potentially exploitable crash. This vulnerability
affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2,
Firefox ESR < 78.15, and Firefox < 93.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                }
            ],
            "version": "85.0.1"
        }
    ],
    "hcc": [
        {
            "ssltest": {
                "description": "",
                "host": "127.0.0.1",
                "sniname": "127.0.0.1",
                "port": "631",
                "protocol": [
                    {
                        "type": "tls",
                        "version": "1.0",
                        "enabled": "1"
                    },
                    {
                        "type": "tls",
                        "version": "1.1",
                        "enabled": "1"
                    },
                    {
                        "type": "tls",
                        "version": "1.2",
                        "enabled": "1"
                    },
                    {
                        "type": "tls",
                        "version": "1.3",
                        "enabled": "1"
                    }
                ],
                "heartbleed": []
            }
        }
    ],
    "hnm": [
        {
            "DestinationMAC": "00:0c:29:68:24:5a",
            "DestinationPort": 50975,
            "AlertType": "ATTACK",
            "GMID": "984a2797-190b-4d28-a5b8-d97597a5bb11",
            "Description": "Network Probe has prevented a suspicious DNS
request to a public server that could contain private data. This is a
potential data exfiltration marker. Data exfiltration is a form of a
security breach that occurs when an individual's or company's data is
copied, transferred, or retrieved from a computer or server without
authorization.",
            "DestinationIp": "192.168.198.204",
            "SourceIp": "192.168.198.203",
            "event_name": "detection",
            "AlertName": "Exploit.DNS.ExfiltrationQuery",
            "TimeCreated": 1637750665615,
            "SourceMAC": "00:0c:29:a3:01:b7",
            "SourcePort": 445
        },
        {
            "DestinationMAC": "00:50:56:b7:57:4f",
            "DestinationPort": 49671,
            "AlertType": "ATTACK",
            "Description": "Network probe has detected a request to a
suspicious DNS domain.",
            "DestinationIp": "10.18.139.78",
            "SourceIp": "10.18.139.58",
            "event_name": "alert",
            "AlertName": "Alert.DNS.DGA.SuspiciousDomain",
            "TimeCreated": 1637750665616,
            "SourceMAC": "00:50:56:b7:5e:a9",
            "SourcePort": 35168
        }
    ]
}
```

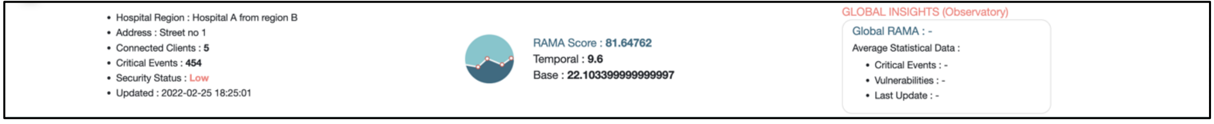
Appendix B – 1st complete version of the RAMA Score Calculator sample output**Erreur ! Source du renvoi introuvable.**.

2.4 *The HEIR Client Graphical Unit Interface*

The HEIR Client GUI (HCG) includes visualisations of information generated by the 1st level services running inside a hospital environment. This information is only available to authorized users belonging to the hospital staff since it contains security-related information of the infrastructure that must be protected. Moreover, HCG fetches information from the HEIR Observatory to be used as a ‘comparison’ of the local aggregated RAMA score and the global one, thus providing users with an idea of how their hospital stands with regards to other infrastructures.

Users accessing the 1st layer of visualisations see the aggregated RAMA scores (RAMA, Base and Temporal) of the Hospital, as generated by the HEIR Aggregator, as well as generic information about the Hospital and its security status (part of the aggregator’s output metadata).

Average statistical data and Global RAMA Score's indicators are retrieved from the Observatory and presented in the top right level of the HCG's page as seen in *Figure 3* below.



- Hospital Region : Hospital A from region B
- Address : Street no 1
- Connected Clients : **5**
- Critical Events : **454**
- Security Status : Low
- Updated : 2022-02-25 18:25:01

RAMA Score : **81.64762**
Temporal : **9.6**
Base : **22.103399999999997**

GLOBAL INSIGHTS (Observatory)

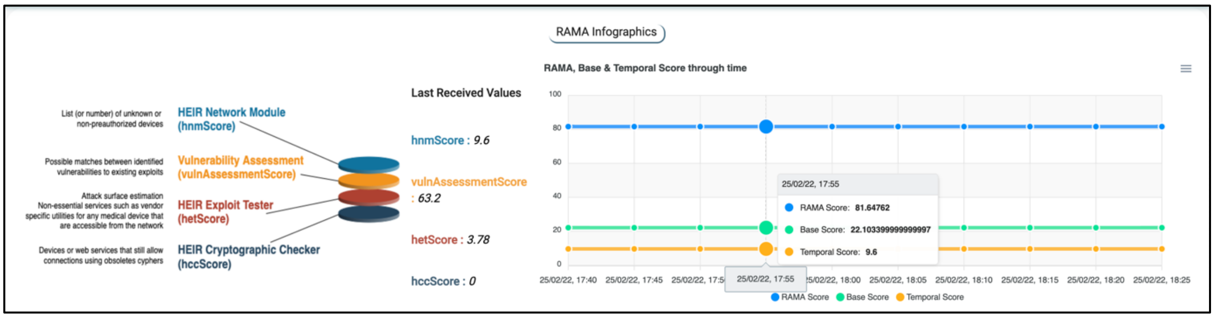
Global RAMA : -

Average Statistical Data :

- Critical Events : -
- Vulnerabilities : -
- Last Update : -

Figure 3. Local and Global RAMA scores

A short description of the modules that contribute to the RAMA scores calculation, along with the corresponding value indicators, are available into the next panel (*Figure 4*). Moreover, 'RAMA Infographics' section includes a multi series line-chart that demonstrates the evolution of the aggregated scores through time, to enhance the end-user's awareness and better monitor the deviations of the scores.



RAMA Infographics

List (or number) of unknown or non-preauthorized devices — HEIR Network Module (hnmScore)

Possible matches between identified vulnerabilities to existing exploits — Vulnerability Assessment (vulnAssessmentScore)

Attack surface estimation Non-essential services such as vendor specific utilities for any medical device that are accessible from the network — HEIR Exploit Tester (hetScore)

Devices or web services that still allow connections using obsoletes cyphers — HEIR Cryptographic Checker (hccScore)

Last Received Values

hnmScore : *9.6*

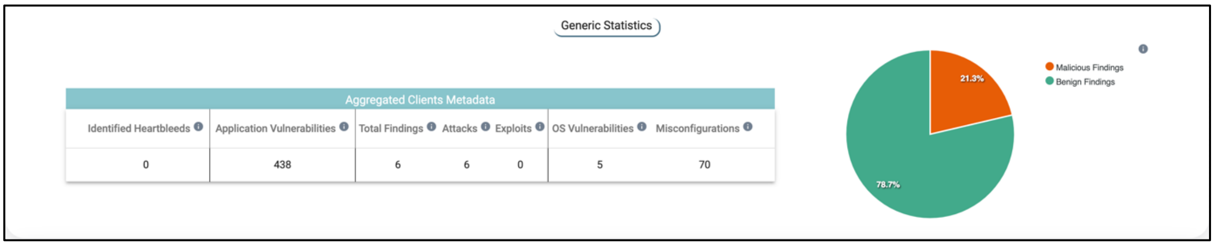
vulnAssessmentScore : *63.2*

hetScore : *3.78*

hccScore : *0*

Figure 4. RAMA sub-scores and Historical RAMA Score evolution

Part of the metadata that Aggregator reports refer to the output of the HEIR Client's embedded modules inside each department. This information is displayed in a tabular view it is categorised based on the source module. Detected application and OS vulnerabilities, captured network related events, active misconfigurations and event analysis results are indicative examples of the current available information (*Figure 5*). The pie-chart concludes the percentage of findings that are malicious.



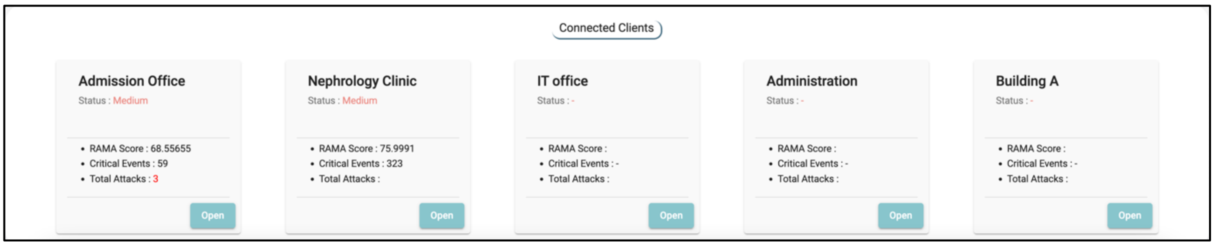
Generic Statistics

Aggregated Clients Metadata

Identified Heartbleeds	Application Vulnerabilities	Total Findings	Attacks	Exploits	OS Vulnerabilities	Misconfigurations
0	438	6	6	0	5	70

Figure 5. Client Statistics and graphical representation

At the bottom of the page users can check the connected departments (HEIR Clients) of the hospital (*Figure 6*). A summary of useful information is displayed and the option to further investigate a selected client is available. ('Open' button). By opening a specific client, user access the Forensics Visualization Toolkit's (FVT) home page. Through the FVT, the end-user can monitor and investigate the connected devices' logged events, check the output of the Anomaly Detection Component (ML), examine the RAMA score and relevant metadata, and more. More details about FVT are described in D2.2.



Connected Clients

Admission Office
Status : Medium

- RAMA Score : 68.55655
- Critical Events : 59
- Total Attacks : 3

Open

Nephrology Clinic
Status : Medium

- RAMA Score : 75.9991
- Critical Events : 323
- Total Attacks :

Open

IT office
Status : -

- RAMA Score :
- Critical Events : -
- Total Attacks :

Open

Administration
Status : -

- RAMA Score :
- Critical Events : -
- Total Attacks :

Open

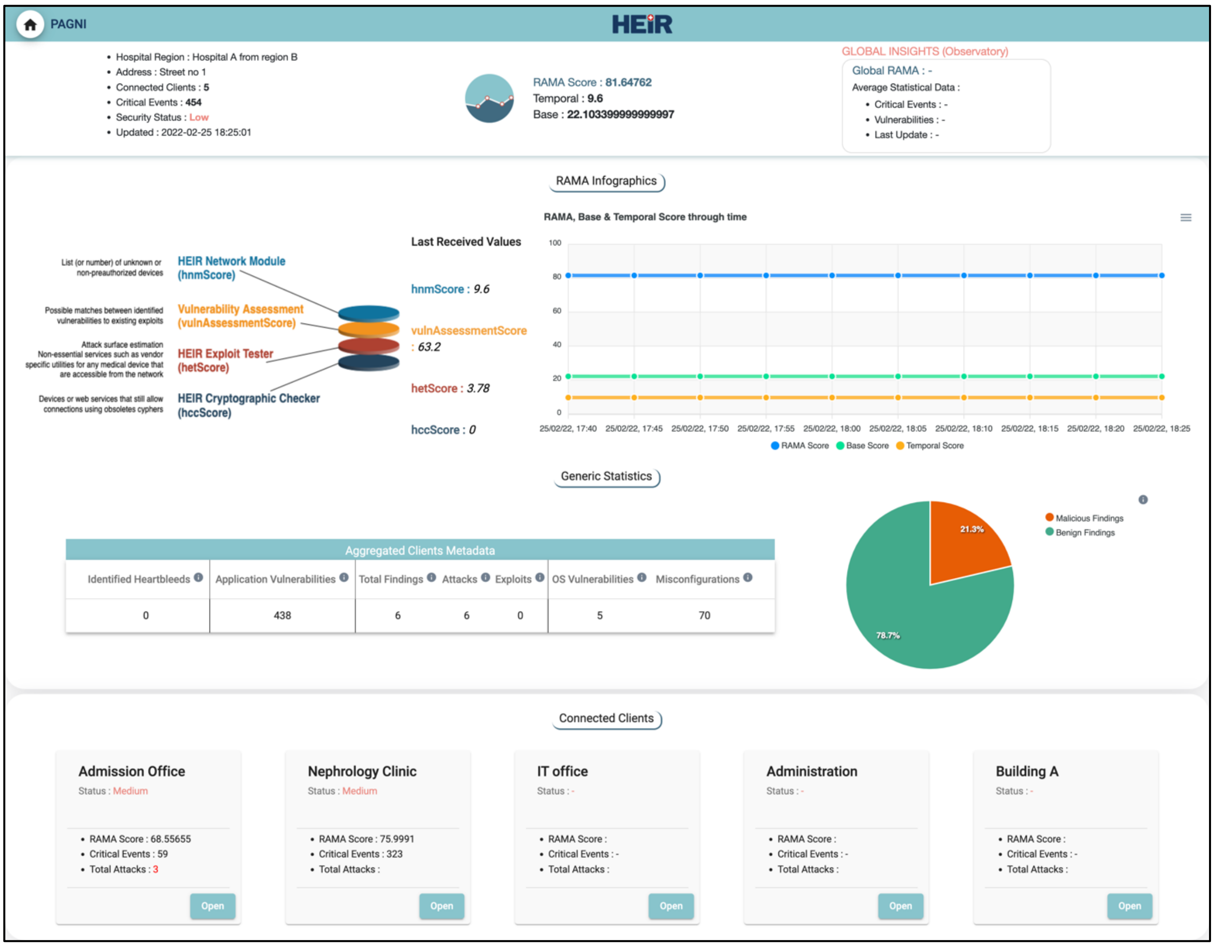
Building A
Status : -

- RAMA Score :
- Critical Events : -
- Total Attacks :

Open

Figure 6. Connected Clients

The complete HCG page is presented in *Figure 7* below.



PAGNI

- Hospital Region : Hospital A from region B
- Address : Street no 1
- Connected Clients : **5**
- Critical Events : **454**
- Security Status : Low
- Updated : 2022-02-25 18:25:01

RAMA Score : **81.64762**
Temporal : **9.6**
Base : **22.103399999999997**

GLOBAL INSIGHTS (Observatory)

Global RAMA : -
Average Statistical Data :

- Critical Events : -
- Vulnerabilities : -
- Last Update : -

RAMA Infographics

List (or number) of unknown or non-preauthorized devices — HEIR Network Module (hnmScore)

Possible matches between identified vulnerabilities to existing exploits — Vulnerability Assessment (vulnAssessmentScore)

Attack surface estimation Non-essential services such as vendor specific utilities for any medical device that are accessible from the network — HEIR Exploit Tester (hetScore)

Devices or web services that still allow connections using obsoletes cyphers — HEIR Cryptographic Checker (hccScore)

Last Received Values

hnmScore : *9.6*

vulnAssessmentScore : *63.2*

hetScore : *3.78*

hccScore : *0*

RAMA, Base & Temporal Score through time

Generic Statistics

Aggregated Clients Metadata

Identified Heartbleeds	Application Vulnerabilities	Total Findings	Attacks	Exploits	OS Vulnerabilities	Misconfigurations
0	438	6	6	0	5	70

Connected Clients

Admission Office
Status : Medium

- RAMA Score : 68.55655
- Critical Events : 59
- Total Attacks : 3

Open

Nephrology Clinic
Status : Medium

- RAMA Score : 75.9991
- Critical Events : 323
- Total Attacks :

Open

IT office
Status : -

- RAMA Score :
- Critical Events : -
- Total Attacks :

Open

Administration
Status : -

- RAMA Score :
- Critical Events : -
- Total Attacks :

Open

Building A
Status : -

- RAMA Score :
- Critical Events : -
- Total Attacks :

Open

Figure 7. Complete page of HEIR Client GUI

2.5 *The HEIR Aggregator*

As described in depth in in "D3.1 – The HEIR 1st layer of services package for the MVP", the HEIR Aggregator is the component of the HEIR framework which compiles the local RAMA scores as well as the Metadata for hospitals operating multiple independent departments, giving a large-scale cybersecurity image for the entire healthcare institution.

In the current version of the – The HEIR 1st layer of services, the HEIR Aggregator has been updated in 2 significant ways:

- Firstly, the HEIR Aggregator will be deployed to all HEIR pilots that contain local RAMA calculators since the HEIR Aggregator has become essentially the component transferring local RAMA scores as well as HEIR Client Metadata from the ElasticSearch storage where they were inserted by the KAFKA connector (*Figure 8* to the HEIR Client Graphical Unit Interface by means of ElasticSearch.

- Secondly, the HEIR Aggregator output JSON schema (Annex B) has been updated to reflect the changes in the local HEIR Client and RAMA calculator outputs. The main changes are regarding the new RAMA scores as well as the added functionalities in the HEIR clients.

As seen in *Figure 8* the HEIR Aggregator is deployed to the pilots' environment as a Docker container which incorporates a ChronJob running every 5 minutes calling the Python procedures that perform the processes necessary for aggregating the local RAMA scores and Metadata, as well as inserting the aggregates to the ElasticSearch storage kept in the pilot environment.

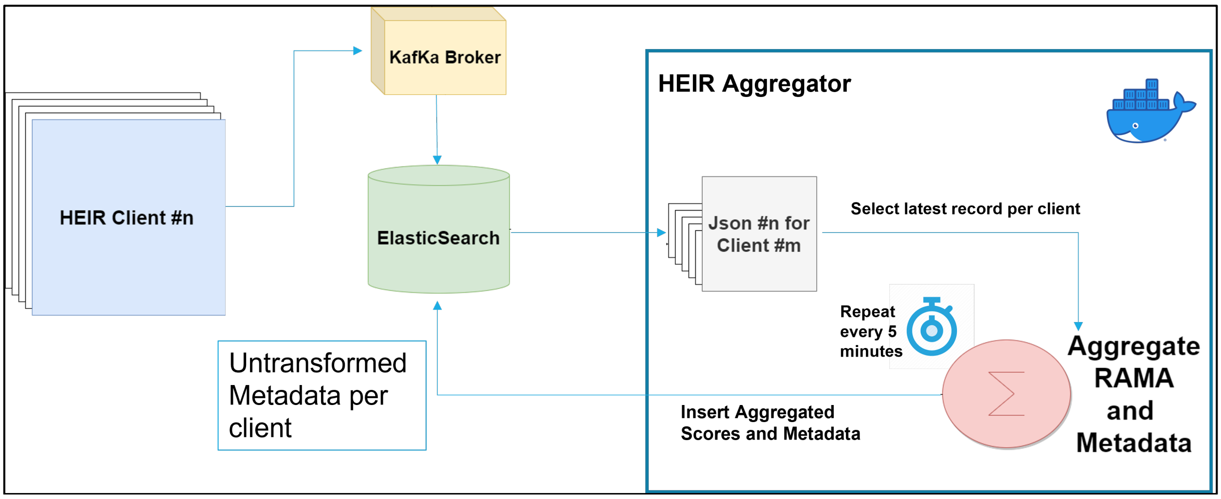

KafKa Broker
HEIR Aggregator
HEIR Client #n
ElasticSearch
Json #n for Client #m
Select latest record per client
Repeat every 5 minutes
Aggregate RAMA and Metadata
Untransformed Metadata per client
Insert Aggregated Scores and Metadata

Figure 8. HEIR Aggregator deployment diagram.

3. The complete version of HEIR’s 1st layer of services package for the Use Cases

PAGNI's PANACEA is a patient management information system (bed management system), providing the health professional with the right information, when needed, in a way that can easily monitor a hospitalisation incident, ensuring a "paperless" environment. At the same time, it enables the treating physician to have a complete picture of his/her patient, as he/she can gather information from all the hospitals of Crete. In more detail, PANACEA is a complete hospital electronic file, accessible from any computer system (PC, tablet, smartphone, etc.)

PANACEA servers are located at the hospital's server room running. For the 1st complete version of services, the 1st layer of services package is deployed within PAGNI's local environment to identify potential issues. The Local RAMA Score will be calculated based on these findings.

The flow of the 1st complete version of scenarios has evolved since the MVP and now it is as follows:

- The Heir Agent (Endpoint component) containing the Vulnerability and Heir Exploit Tester is deployed on Endpoints.

- Instead of a scheduled task the Heir Agent run as a service that is less intrusive and more silent. The tool will generate an event (report) regarding misconfiguration risks and application vulnerability assessment.

- The generated event (report) will be emitted to the message broker to the central HEIR Client (now as a separated component) where is normalized and aggregated and then submitted by the message broker to the RAMA Score Calculator.

- The RAMA Score calculator receives the alerts, computes the RAMA Score in real-time, provides the score alongside metadata through the KAFKA message broker.

- Lastly, the RAMA score and its metadata are being stored in an Elasticsearch database so that it can be retrieved from the HEIR Aggregator and visualised through the HEIR GUI.

4. Conclusion

This document explained the design and definition of the HEIR 1st layer of services package: the 1st complete version. The current status of the services package has been firstly conceptualised following inputs from deliverables D3.1, D4.1 and D5.2. Then, the technical advancements made between M12 and M18 were illustrated within the document complemented by the showcase of how the current version impacts the use-cases. Lastly, the three Annexes present the samples output.

The next steps include continuous updating of the HEIR 1st layer of services considering the evaluators input that will be received during the evaluation period, as well as the ongoing work within the WP3 and connecting WPs such as 4 and 5. Further internal updates will be deployed across the modules based on the use-cases particularities, to achieve a homogenous 1st layer of services.

The next phase of reporting the WP3 activities will be described by "D3.3: The HEIR 1st layer of services package, the final version", which will serve as an instrument to present the final configuration for components like the HEIR Client, the local RAMA Score Calculator the HEIR Client Graphical Unit and the HEIR Aggregator.

5. Appendix A – 1st complete version of the HEIR Client sample output

```
{
    "clientId": 1234,
    "connected_clients": 1,
    "het": [
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Verifies the local group policy settings for
User Configuration\\Administrative Templates\\System\\Ctrl+Alt+Del
Options\\Remove Task Manager. When Remove Task Manager is enabled, the
endpoint is vulnerable to security threats. Since Task Manager can list and
terminate currently running processes, some malware may disable it to
prevent themselves from being closed.",
            "integrity": "None",
            "name": "Task Manager",
            "score": 25,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Verifies if Windows requires account sign-in.
When the user accounts sign-in is disabled, Windows stores the user
passwords in the registry database, making possible to bypass the password
screen during logon.",
            "integrity": "None",
            "name": "Auto Logon",
            "score": 25,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Low",
            "description": "Verifies the local security policy option User
Account Control: Run all administrators in Admin Approval Mode. This
setting controls the behavior of all UAC policy settings for the endpoint.
UAC (User Account Control) is a security feature that helps preventing
unauthorized changes to the OS by potentially harmful programs. UAC
requires administrator authorization for actions like installing a program
or modifying system settings. When UAC is set to Never notify, the system
is more vulnerable to malware.",
            "integrity": "Low",
            "name": "UAC Off",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Low",
            "description": "Verifies the configuration for User Account
Control policy and registry settings, to check if these comply with the
default recommended settings. The policy settings are located in Security
Settings\\Local Policies\\Security Options, in the Local Security Policy
app.",
            "integrity": "Low",
            "name": "UAC Insecure",
            "score": 30,
            "triggered": true,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Verifies the local group policy Turn off Data
Execution Prevention for Explorer, located in Computer
Configuration\\Administrative Templates\\Windows Components\\File Explorer.
Disabling data execution prevention can allow certain legacy plug-in
applications to function without terminating Explorer.",
            "integrity": "Low",
            "name": "Explorer Data Execution Prevention",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Verifies the local group policy Turn off heap
termination on corruption, located in Computer
Configuration\\Administrative Templates\\Windows Components\\File Explorer.
Disabling heap termination on corruption can allow certain legacy plug-in
applications to function without terminating Explorer immediately, although
Explorer may still terminate unexpectedly later.",
            "integrity": "Low",
            "name": "Heap Termination on Corruption",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Verifies the local group policy Do not allow
passwords to be saved, located in Computer Configuration\\Administrative
Templates\\Windows Components\\Remote Desktop Services\\Remote Desktop
Connection Client. This policy controls whether passwords can be saved on
this computer from Remote Desktop Connection.  - If you enable this
setting, the password saving checkbox in Remote Desktop Connection will be
disabled and users will no longer be able to save passwords. When a user
opens an RDP file using Remote Desktop Connection and saves his settings,
any password that previously existed in the RDP file will be deleted.",
            "integrity": "Low",
            "name": "Save Passwords from RDP",
            "score": 50,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Verifies the local group policy Do not allow
drive redirection, located in Computer Configuration\\Administrative
Templates\\Windows Components\\Remote Desktop Services\\Remote Desktop
Session Host\\Device and Resource Redirection. This policy setting
specifies whether to prevent the mapping of client drives in a Remote
Desktop Services session (drive redirection). By default, an RD Session
```

```
Host server maps client drives automatically upon connection. Mapped drives
appear in the session folder tree in File Explorer or Computer in the
format &lt;driveletter&gt; on &lt;computername&gt;. You can use this policy
setting to override this behavior.  - If you enable this policy setting,
client drive redirection is not allowed in Remote Desktop Services
sessions, and Clipboard file copy redirection is not allowed on computers
running Windows Server 2003, Windows 8, and Windows XP.",
            "integrity": "Low",
            "name": "Drive Redirection",
            "score": 50,
            "triggered": true,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Checks the Macro settings for Office Word 16,
located in File\\Options\\Trust Center\\Trust Center Settings\\Macro
Settings. Disable all macros without notification - Macros and security
alerts about macros are disabled. Disable all macros with notification -
Macros are disabled, but security alerts will be triggered if macros are
present. Disable all macros except digitally signed macros - Macros are
disabled, but security alerts will be triggered if macros are present.
However, for macros digitally signed by a trusted publisher, these will run
if the trust access for that publisher has been enabled. Enable all macros
(not recommended, potentially dangerous code can run) - All macros run.
This setting makes your computer vulnerable to potentially malicious code.
Trust access to the VBA project object model.",
            "integrity": "Medium",
            "name": "Office Word 16 Macro",
            "score": 55,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Checks the Macro settings for Office Excel 16,
located in File\\Options\\Trust Center\\Trust Center Settings\\Macro
Settings. Disable all macros without notification - Macros and security
alerts about macros are disabled. Disable all macros with notification -
Macros are disabled, but security alerts will be triggered if macros are
present. Disable all macros except digitally signed macros - Macros are
disabled, but security alerts will be triggered if macros are present.
However, for macros digitally signed by a trusted publisher, these will run
if the trust access for that publisher has been enabled. Enable all macros
(not recommended, potentially dangerous code can run) - All macros run.
This setting makes your computer vulnerable to potentially malicious code.
Trust access to the VBA project object model.",
            "integrity": "Medium",
            "name": "Office Excel 16 Macro",
            "score": 55,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Medium",
            "description": "Checks the Macro settings for Office Outlook
16, located in File\\Options\\Trust Center\\Trust Center Settings\\Macro
Settings. Disable all macros without notification - Macros and security
```

```
alerts about macros are disabled. Disable all macros with notification -
Macros are disabled, but security alerts will be triggered if macros are
present. Disable all macros except digitally signed macros - Macros are
disabled, but security alerts will be triggered if macros are present.
However, for macros digitally signed by a trusted publisher, these will run
if the trust access for that publisher has been enabled. Enable all macros
(not recommended, potentially dangerous code can run) - All macros run.
This setting makes your computer vulnerable to potentially malicious code.
Trust access to the VBA project object model.",
            "integrity": "Medium",
            "name": "Office Outlook 16 Macro",
            "score": 55,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "Low",
            "description": "Checks the number of local administrators on
the machine.",
            "integrity": "None",
            "name": "Too many local administrators",
            "score": 40,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "High",
            "description": "Checks the existence of shared folders with
read access for the Everyone group. The Everyone group includes all users
who have logged in with a password (members of the Authenticated Users
group) as well as built-in, non-password protected accounts such as Guest,
and several other built-in security accounts like SERVICE, LOCAL_SERVICE,
NETWORK_SERVICE, and others. A Guest account is a built-in account on a
Windows system that is disabled by default.  - If enabled, it allows anyone
to login without a password.",
            "integrity": "None",
            "name": "SMB Shared Everyone Read",
            "score": 20,
            "triggered": true,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "None",
            "description": "Checks the existence of shared folders with
write access for the Everyone group. The Everyone group includes all users
who have logged in with a password (members of the Authenticated Users
group) as well as built-in, non-password protected accounts such as Guest,
and several other built-in security accounts like SERVICE, LOCAL_SERVICE,
NETWORK_SERVICE, and others. A Guest account is a built-in account on a
Windows system that is disabled by default.  - If enabled, it allows anyone
to login without a password.",
            "integrity": "Medium",
            "name": "SMB Shared Everyone Write",
            "score": 25,
            "triggered": false,
            "type": "MisConfiguration"
        },
        {
            "availability": "None",
            "confidentiality": "High",
            "description": "Verifies if regular users are allowed to read
the Security Account Manager (SAM) data. Non-admin users should not be
allowed to read critical files, but a vulnerability (known as HiveNightmare
or SeriousSam) has been discovered in Windows 11 and Windows 10 version
1809 and above, which involved a \"bad\" ACL being set on the
%SystemRoot%\\System32\\Config folder, making it possible for regular users
to acces the SAM, SYSTEM, SECURITY and other critical files.",
            "integrity": "Medium",
            "name": "SAM File readable by users",
            "score": 80,
            "triggered": false,
            "type": "Vulnerability"
        }
    ],
    "hospitalId": 5678,
    "hospital_address": "Street no 1",
    "hospital_region": "Hospital A from region B",
    "host_name": "HOST-L2",
    "host_os": "Windows 10",
    "machine_id":
"3119BFD93119E3AB3119D0123119960B3119B2ED3119FDE63119DF543119C5BB3119FC3531
1994B33119DB3C3119D9C23119A1363119BCC73119BDB63119F25A",
    "scan_id": "00943c780094363d00940dfd00944745",
    "scan_status": "finished",
    "vulnerabilityAssessment": [
        {
            "application_name": "Mozilla Firefox",
            "cves": [
                {
                    "cve": "CVE-2007-3670",
                    "description": "Argument injection vulnerability in
Microsoft Internet Explorer, when running on systems with Firefox installed
and certain URIs registered, allows remote attackers to conduct cross-
browser scripting attacks and execute arbitrary commands via shell
metacharacters in a (1) FirefoxURL or (2) FirefoxHTML URI, which are
inserted into the command line that is created when invoking firefox.exe.
NOTE: it has been debated as to whether the issue is in Internet Explorer
or Firefox. As of 20070711, it is CVE's opinion that IE appears to be
failing to properly delimit the URL argument when invoking Firefox, and
this issue could arise with other protocol handlers in IE as well. However,
Mozilla has stated that it will address the issue with a
\\\\\\\\\\\\\\\"defense in depth\\\\\\\\\\\\\\\" fix that will
\\\\\\\\\\\\\\\"prevent IE from sending Firefox malicious
data.\\\\\\\\\\\\\\\"",
                    "publish_date": "2007-07-10T19:30Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2011-0064",
                    "description": "The hb_buffer_ensure function in hb-
buffer.c in HarfBuzz, as used in Pango 1.28.3, Firefox, and other products,
does not verify that memory reallocations succeed, which allows remote
attackers to cause a denial of service (NULL pointer dereference and
application crash) or possibly execute arbitrary code via crafted OpenType
font data that triggers use of an incorrect index.",
                    "publish_date": "2011-03-07T21:00Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2011-3389",
                    "description": "The SSL protocol, as used in certain
configurations in Microsoft Windows and Microsoft Internet Explorer,
Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by
using CBC mode with chained initialization vectors, which allows man-in-
the-middle attackers to obtain plaintext HTTP headers via a blockwise
chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with
JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java
URLConnection API, or (3) the Silverlight WebClient API, aka a
\\\\\\\\\\\\\\\"BEAST\\\\\\\\\\\\\\\" attack.",
                    "publish_date": "2011-09-06T19:55Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2015-4000",
                    "description": "The TLS protocol 1.2 and earlier, when
a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does
not properly convey a DHE_EXPORT choice, which allows man-in-the-middle
attackers to conduct cipher-downgrade attacks by rewriting a ClientHello
with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with
DHE_EXPORT replaced by DHE, aka the \\\\\\\\\\\\\\\"Logjam\\\\\\\\\\\\\\\"
issue.",
                    "publish_date": "2015-05-21T00:59Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23987",
                    "description": "Mozilla developers and community
members reported memory safety bugs present in Firefox 86 and Firefox ESR
78.8. Some of these bugs showed evidence of memory corruption and we
presume that with enough effort some of these could have been exploited to
run arbitrary code. This vulnerability affects Firefox ESR < 78.9, Firefox
< 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23988",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 86. Some of these bugs showed evidence of
memory corruption and we presume that with enough effort some of these
could have been exploited to run arbitrary code. This vulnerability affects
Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23984",
                    "description": "A malicious extension could have opened
a popup window lacking an address bar. The title of the popup lacking an
address bar should not be fully controllable, but in this situation was.
This could have been used to spoof a website and attempt to trick the user
into providing credentials. This vulnerability affects Firefox ESR < 78.9,
Firefox < 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23986",
                    "description": "A malicious extension with the 'search'
permission could have installed a new search engine whose favicon
```

```
referenced a cross-origin URL. The response to this cross-origin request
could have been read by the extension, allowing a same-origin policy bypass
by the extension, which should not have cross-origin permissions. This
cross-origin request was made without cookies, so the sensitive information
disclosed by the violation was limited to local-network resources or
resources that perform IP-based authentication. This vulnerability affects
Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23981",
                    "description": "A texture upload of a Pixel Buffer
Object could have confused the WebGL code to skip binding the buffer used
to unpack it, resulting in memory corruption and a potentially exploitable
information leak or crash. This vulnerability affects Firefox ESR < 78.9,
Firefox < 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-23982",
                    "description": "Using techniques that built on the
slipstream research, a malicious webpage could have scanned both an
internal network's hosts as well as services running on the user's local
machine utilizing WebRTC connections. This vulnerability affects Firefox
ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23983",
                    "description": "By causing a transition on a parent
node by removing a CSS rule, an invalid property for a marker could have
been applied, resulting in memory corruption and a potentially exploitable
crash. This vulnerability affects Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23985",
                    "description": "If an attacker is able to alter
specific about:config values (for example malware running on the user's
computer), the Devtools remote debugging feature could have been enabled in
a way that was unnoticable to the user. This would have allowed a remote
attacker (able to make a direct network connection to the victim) to
monitor the user's browsing activity and (plaintext) network traffic. This
was addressed by providing a visual cue when Devtools has an open network
socket. This vulnerability affects Firefox < 87.",
                    "publish_date": "2021-03-31T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29968",
                    "description": "When drawing text onto a canvas with
WebRender disabled, an out of bounds read could occur. *This bug only
affects Firefox on Windows. Other operating systems are unaffected.*. This
vulnerability affects Firefox < 89.0.1.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-29967",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 88 and Firefox ESR 78.11. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR <
78.11.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29966",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 88. Some of these bugs showed evidence of
memory corruption and we presume that with enough effort some of these
could have been exploited to run arbitrary code. This vulnerability affects
Firefox < 89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29947",
                    "description": "Mozilla developers and community
members reported memory safety bugs present in Firefox 87. Some of these
bugs showed evidence of memory corruption and we presume that with enough
effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29946",
                    "description": "Ports that were written as an integer
overflow above the bounds of a 16-bit integer could have bypassed port
blocking restrictions when used in the Alt-Svc header. This vulnerability
affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29964",
                    "description": "A locally-installed hostile program
could send `WM_COPYDATA` messages that Firefox would process incorrectly,
leading to an out-of-bounds read. *This bug only affects Firefox on
Windows. Other operating systems are unaffected.*. This vulnerability
affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-29961",
                    "description": "When styling and rendering an oversized
`<select>` element, Firefox did not apply correct clipping which allowed an
attacker to paint over the user interface. This vulnerability affects
Firefox < 89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29960",
                    "description": "Firefox used to cache the last filename
used for printing a file. When generating a filename for printing, Firefox
usually suggests the web page title. The caching and suggestion techniques
combined may have lead to the title of a website visited during private
browsing mode being stored on disk. This vulnerability affects Firefox <
89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29959",
                    "description": "When a user has already allowed a
website to access microphone and camera, disabling camera sharing would not
fully prevent the website from re-enabling it without an additional prompt.
This was only possible if the website kept recording with the microphone
until re-enabling the camera. This vulnerability affects Firefox < 89.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29955",
                    "description": "A transient execution vulnerability,
named Floating Point Value Injection (FPVI) allowed an attacker to leak
arbitrary memory addresses and may have also enabled JIT type confusion
attacks. (A related vulnerability, Speculative Code Store Bypass (SCSB),
did not affect Firefox.). This vulnerability affects Firefox ESR < 78.9 and
Firefox < 87.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 26
                },
                {
                    "cve": "CVE-2021-29951",
                    "description": "The Mozilla Maintenance Service granted
SERVICE_START access to BUILTIN|Users which, in a domain network, grants
normal remote users access to start or stop the service. This could be used
to prevent the browser update service from operating (if an attacker
spammed the 'Stop' command); but also exposed attack surface in the
maintenance service. *Note: This issue only affected Windows operating
systems older than Win 10 build 1709. Other operating systems are
unaffected.*. This vulnerability affects Thunderbird < 78.10.1, Firefox <
87, and Firefox ESR < 78.10.1.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 64
                },
                {
                    "cve": "CVE-2021-29944",
                    "description": "Lack of escaping allowed HTML injection
when a webpage was viewed in Reader View. While a Content Security Policy
prevents direct code execution, HTML injection is still possible. *Note:
This issue only affected Firefox for Android. Other operating systems are
unaffected.*. This vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-24002",
                    "description": "When a user clicked on an FTP URL
containing encoded newline characters (%0A and %0D), the newlines would
have been interpreted as such and allowed arbitrary commands to be sent to
the FTP server. This vulnerability affects Firefox ESR < 78.10, Thunderbird
< 78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-24001",
                    "description": "A compromised content process could 
have performed session history manipulations it should not have been able 
to due to testing infrastructure that was not restricted to testing-only 
configurations. This vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-24000",
                    "description": "A race condition with 
requestPointerLock() and setTimeout() could have resulted in a user 
interacting with one tab when they believed they were on a separate tab. In 
conjunction with certain elements (such as &lt;input 
type=\\\\\\\\\\\\\\\"file\\\\\\\\\\\\\\\"&gt;) this could have led to an 
attack where a user was confused about the origin of the webpage and 
potentially disclosed information they did not intend to. This 
vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 26
                },
                {
                    "cve": "CVE-2021-23999",
                    "description": "If a Blob URL was loaded through some 
unusual user interaction, it could have been loaded by the System Principal 
and granted additional privileges that should not be granted to web 
content. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 
78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23998",
                    "description": "Through complicated navigations with 
new windows, an HTTP page could have inherited a secure lock icon from an 
HTTPS page. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 
78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23996",
                    "description": "By utilizing 3D CSS in conjunction with 
Javascript, content could have been rendered outside the webpage's 
viewport, resulting in a spoofing attack that could have been used for 
phishing or other attacks on a user. This vulnerability affects Firefox < 
88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-23997",
                    "description": "Due to unexpected data type 
conversions, a use-after-free could have occurred when interacting with the 
font cache. We presume that with enough effort this could have been 
exploited to run arbitrary code. This vulnerability affects Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-23995",
                    "description": "When Responsive Design Mode was
enabled, it used references to objects that were previously freed. We
presume that with enough effort this could have been exploited to run
arbitrary code. This vulnerability affects Firefox ESR < 78.10, Thunderbird
< 78.10, and Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 50
                },
                {
                    "cve": "CVE-2021-23994",
                    "description": "A WebGL framebuffer was not initialized
early enough, resulting in memory corruption and an out of bound write.
This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and
Firefox < 88.",
                    "publish_date": "2021-06-24T14:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29989",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox
< 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29988",
                    "description": "Firefox incorrectly treated an inline
list-item element as a block element, resulting in an out of bounds read or
memory corruption, and a potentially exploitable crash. This vulnerability
affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and
Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29987",
                    "description": "After requesting multiple permissions,
and closing the first permission panel, subsequent permission panels will
be displayed in a different position but still record a click in the
default location, making it possible to trick a user into accepting a
permission they did not want to. *This bug only affects Firefox on Linux.
Other operating systems are unaffected.*. This vulnerability affects
Firefox < 91 and Thunderbird < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29986",
                    "description": "A suspected race condition when calling
getaddrinfo led to memory corruption and a potentially exploitable crash.
*Note: This issue only affected Linux operating systems. Other operating
systems are unaffected.* This vulnerability affects Thunderbird < 78.13,
Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29985",
                    "description": "A use-after-free vulnerability in media
channels could have led to memory corruption and a potentially exploitable
crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91,
Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29984",
                    "description": "Instruction reordering resulted in a
sequence of instructions that would cause an object to be incorrectly
considered during garbage collection. This led to memory corruption and a
potentially exploitable crash. This vulnerability affects Thunderbird <
78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29983",
                    "description": "Firefox for Android could get stuck in
fullscreen mode and not exit it even after normal interactions that should
cause it to exit. *Note: This issue only affected Firefox for Android.
Other operating systems are unaffected.*. This vulnerability affects
Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29982",
                    "description": "Due to incorrect JIT optimization, we
incorrectly interpreted data from the wrong type of object, resulting in
the potential leak of a single bit of memory. This vulnerability affects
Firefox < 91 and Thunderbird < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29981",
                    "description": "An issue present in lowering/register
allocation could have led to obscure but deterministic register confusion
failures in JITted code that would lead to a potentially exploitable crash.
This vulnerability affects Firefox < 91 and Thunderbird < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29980",
                    "description": "Uninitialized memory in a canvas object
could have caused an incorrect free() leading to memory corruption and a
potentially exploitable crash. This vulnerability affects Thunderbird <
78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-29990",
                    "description": "Mozilla developers and community
members reported memory safety bugs present in Firefox 90. Some of these
bugs showed evidence of memory corruption and we presume that with enough
effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 91.",
                    "publish_date": "2021-08-17T20:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38501",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR <
91.2.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38500",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR
< 91.2, Firefox ESR < 78.15, and Firefox < 93.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38499",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 92. Some of these bugs showed evidence of
memory corruption and we presume that with enough effort some of these
could have been exploited to run arbitrary code. This vulnerability affects
Firefox < 93.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38498",
                    "description": "During process shutdown, a document
could have caused a use-after-free of a languages service object, leading
to memory corruption and a potentially exploitable crash. This
vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR <
91.2.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 50
                },
                {
                    "cve": "CVE-2021-38497",
                    "description": "Through use of reportValidity() and
window.open(), a plain-text validation message could have been overlaid on
another origin, leading to possible user confusion and spoofing attacks.
This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox
ESR < 91.2.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-38494",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 91. Some of these bugs showed evidence of
memory corruption and we presume that with enough effort some of these
could have been exploited to run arbitrary code. This vulnerability affects
Firefox < 92.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38493",
                    "description": "Mozilla developers reported memory
safety bugs present in Firefox 91 and Firefox ESR 78.13. Some of these bugs
showed evidence of memory corruption and we presume that with enough effort
some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox ESR < 78.14, Thunderbird < 78.14, and Firefox
< 92.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                },
                {
                    "cve": "CVE-2021-38492",
                    "description": "When delegating navigations to the
operating system, Firefox would accept the `mk` scheme which might allow
attackers to launch pages and execute scripts in Internet Explorer in
unprivileged mode. *This bug only affects Firefox for Windows. Other
operating systems are unaffected.*. This vulnerability affects Firefox <
92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and
Firefox ESR < 91.1.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-38491",
                    "description": "Mixed-content checks were unable to
analyze opaque origins which led to some mixed content being loaded. This
vulnerability affects Firefox < 92.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 42
                },
                {
                    "cve": "CVE-2021-29991",
                    "description": "Firefox incorrectly accepted a newline
in a HTTP/3 header, interpretting it as two separate headers. This allowed
for a header splitting attack against servers using HTTP/3. This
vulnerability affects Firefox < 91.0.1 and Thunderbird < 91.0.1.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 57
                },
                {
                    "cve": "CVE-2021-38496",
                    "description": "During operations on MessageTasks, a
task may have been removed while it was still scheduled, resulting in
memory corruption and a potentially exploitable crash. This vulnerability
affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2,
Firefox ESR < 78.15, and Firefox < 93.",
                    "publish_date": "2021-11-03T01:15Z",
                    "score": 67
                }
            ],
            "version": "85.0.1"
```

```
        }
    ],
    "hcc": [
        {
            "ssltest": {
                "description": "",
                "host": "127.0.0.1",
                "sniname": "127.0.0.1",
                "port": "631",
                "protocol": [
                    {
                        "type": "tls",
                        "version": "1.0",
                        "enabled": "1"
                    },
                    {
                        "type": "tls",
                        "version": "1.1",
                        "enabled": "1"
                    },
                    {
                        "type": "tls",
                        "version": "1.2",
                        "enabled": "1"
                    },
                    {
                        "type": "tls",
                        "version": "1.3",
                        "enabled": "1"
                    }
                ],
                "heartbleed": []
            }
        }
    ],
    "hnm": [
        {
            "DestinationMAC": "00:0c:29:68:24:5a",
            "DestinationPort": 50975,
            "AlertType": "ATTACK",
            "GMID": "984a2797-190b-4d28-a5b8-d97597a5bb11",
            "Description": "Network Probe has prevented a suspicious DNS
request to a public server that could contain private data. This is a
potential data exfiltration marker. Data exfiltration is a form of a
security breach that occurs when an individual's or company's data is
copied, transferred, or retrieved from a computer or server without
authorization.",
            "DestinationIp": "192.168.198.204",
            "SourceIp": "192.168.198.203",
            "event_name": "detection",
            "AlertName": "Exploit.DNS.ExfiltrationQuery",
            "TimeCreated": 1637750665615,
            "SourceMAC": "00:0c:29:a3:01:b7",
            "SourcePort": 445
        },
        {
            "DestinationMAC": "00:50:56:b7:57:4f",
            "DestinationPort": 49671,
            "AlertType": "ATTACK",
            "Description": "Network probe has detected a request to a
suspicious DNS domain.",
            "DestinationIp": "10.18.139.78",
            "SourceIp": "10.18.139.58",
            "event_name": "alert",
            "AlertName": "Alert.DNS.DGA.SuspiciousDomain",
            "TimeCreated": 1637750665616,
            "SourceMAC": "00:50:56:b7:5e:a9",
            "SourcePort": 35168
        }
    ]
}
```

6. Appendix B – 1st complete version of the RAMA Score Calculator sample output

```
  {
    "temporalScore": {
        "temporalScore": 16,
        "hnmScore": 16,
        "siemScore": 0
    },
    "metadata": {
        "hospital_region": "Hospital A from region B",
        "clientId": 1234,
        "numberOfCriticalEvents": 58,
        "connected_clients": "1",
        "machine_id":
"3119BFD93119E3AB3119D0123119960B3119B2ED3119FDE63119DF543119C5BB3119FC3531
1994B33119DB3C3119D9C23119A1363119BCC73119BDB63119F25A",
        "hetMetadata": {
            "numberOfMaliciousFindings": 3,
            "percentageOfBenignFindings": 80,
            "noOfOSVulnerabilities": 1,
            "percentageOfMaliciousFindings": 20,
            "noOfMisconfigurations": 14,
            "numberOfBenignFindings": 12,
            "hetVector": "C:H/I:L/A:N"
        },
        "indicators": {
            "vaScore": 100,
            "hnmScore": 16,
            "hccScore": 10,
            "hetScore": 3.45,
            "id": 1,
            "facilitatorScore": 0,
            "calculated": "2022-02-03 18:59:34.893"
        },
        "vulnerabilityAssessmentAggregatedMetadata": {
            "vulnerabilityAssessmentMetadata": [{
                "application_name": "Mozilla Firefox",
                "noOfVulnerabilities": 55,
                "vulnerabilities": [
                    "CVE-2021-29981",
                    "CVE-2021-38497",
                    "CVE-2021-23982",
                    "CVE-2021-29946",
                    "CVE-2021-23981",
                    "CVE-2021-29959",
                    "CVE-2021-38501",
                    "CVE-2021-23999",
                    "CVE-2011-3389",
                    "CVE-2021-23986",
                    "CVE-2021-29964",
                    "CVE-2021-29991",
                    "CVE-2021-23983",
                    "CVE-2021-23994",
                    "CVE-2021-38496",
                    "CVE-2021-23984",
                    "CVE-2007-3670",
                    "CVE-2021-29986",
                    "CVE-2021-23998",
                    "CVE-2021-38492",
                    "CVE-2021-29967",
                    "CVE-2021-29980",
                    "CVE-2021-29984",
                    "CVE-2021-29988",
                    "CVE-2021-23987",
                    "CVE-2021-24002",
                    "CVE-2021-23996",
                    "CVE-2021-29951",
                    "CVE-2015-4000",
                    "CVE-2021-29955",
                    "CVE-2021-29990",
                    "CVE-2021-24000",
                    "CVE-2021-38491",
                    "CVE-2021-29985",
                    "CVE-2021-29982",
                    "CVE-2021-24001",
                    "CVE-2021-23997",
                    "CVE-2021-29987",
                    "CVE-2011-0064",
                    "CVE-2021-29960",
                    "CVE-2021-29944",
                    "CVE-2021-38493",
                    "CVE-2021-38494",
                    "CVE-2021-29989",
                    "CVE-2021-29983",
                    "CVE-2021-29968",
                    "CVE-2021-29966",
                    "CVE-2021-23988",
                    "CVE-2021-38499",
                    "CVE-2021-23985",
                    "CVE-2021-29947",
                    "CVE-2021-29961",
                    "CVE-2021-23995",
                    "CVE-2021-38500",
                    "CVE-2021-38498"
                ]
            }],
            "totalNoOfVulnerabilities": 55,
            "top10Vulnerabilities": {
                "CVE-2021-23999": 67,
                "CVE-2021-29981": 67,
                "CVE-2021-29980": 67,
                "CVE-2021-38496": 67,
                "CVE-2021-29986": 67,
                "CVE-2021-29984": 67,
                "CVE-2021-29946": 67,
                "CVE-2021-38501": 67,
                "CVE-2021-29967": 67,
                "CVE-2021-23994": 67
            }
        },
        "hnmMetadata": {
            "numberOfExploits": 0,
            "hnmMetadata": [
                {
                    "destinationPort": 49671,
                    "destinationIp": "10.18.139.78",
                    "sourcePort": 35168,
                    "sourceIp": "10.18.139.58",
                    "description": "Network probe has detected a request to
a suspicious DNS domain."
                },
                {
                    "destinationPort": 50975,
                    "destinationIp": "192.168.198.204",
                    "sourcePort": 445,
                    "sourceIp": "192.168.198.203",
                    "description": "Network Probe has prevented a
suspicious DNS request to a public server that could contain private data.
This is a potential data exfiltration marker. Data exfiltration is a form
of a security breach that occurs when an individual's or company's data is
copied, transferred, or retrieved from a computer or server without
authorization."
                }
            ],
            "numberOfAttacks": 2,
            "totalHNMFindings": 2
        },
        "hospitalId": 5678,
        "hccMetadata": {
            "identifiedHeartbleeds": ["TLSv1.2"],
            "numberOfIdentifiedHeartbleeds": 1
        },
        "hospital_address": "Street no 1",
        "host_name": "test"
    },
    "clientId": 1234,
    "hospitalId": 5678,
    "ramaScore": 68.99305,
    "created": "2022-02-03 18:59:34.901",
    "clientStatus": "Medium",
    "baseScore": {
        "vulnerabilityAssessmentScore": 100,
        "hccScore": 10,
        "hetScore": 3.45,
        "baseScore": 37.4385
    }
}
```

7. Appendix C – 1st complete version of the RAMA Score Calculator sample output

```
{
          "hospitalId" : 5678,
          "hospital_address" : "Street no 1",
          "hospital_region" : "Hospital A from region B",
          "clientIdList" : [
            1234,
            1,
            7,
            2,
            3
          ],
          "noOfClients" : 5,
          "created" : "2022-02-27 17:05:01",
          "ramaScore" : 81.64762,
          "cyberSecurityStatus" : "Low",
          "temporalScore" : 9.6,
          "hnmScore" : 9.6,
          "siemScore" : 0.0,
          "baseScore" : 22.103399999999997,
          "vulnerabilityAssessmentScore" : 63.2,
          "hccScore" : 0.0,
          "hetScore" : 3.78,
          "facilitatorScore" : 0.0,
          "numberOfCriticalEvents" : 454,
          "numberOfIdentifiedHeartbleeds" : 0,
          "noOfOSVulnerabilities" : 5,
          "noOfMisconfigurations" : 70,
          "numberOfBenignFindings" : 59,
          "numberOfMaliciousFindings" : 16,
          "percentageOfBenignFindings" : 78.66666666666667,
          "percentageOfMaliciousFindings" : 21.333333333333332,
          "noOfAppVulnerabilities" : 438,
          "totalHNMFindings" : 6,
          "numberOfAttacks" : 6,
          "numberOfExploits" : 0,
          "top10Vulnerabilities" : "[[\"CVE-2018-4944\", 100], [\"CVE-2018-
4877\", 100], [\"CVE-2018-15982\", 100], [\"CVE-2017-3112\", 100], [\"CVE-
2017-3099\", 100], [\"CVE-2017-3082\", 100], [\"CVE-2017-3076\", 100],
[\"CVE-2017-3075\", 100], [\"CVE-2017-11225\", 100], [\"CVE-2017-11213\",
100], [\"CVE-2021-3517\", 75]]",
          "clientJsonList" : "[{\"hospitalId\": 5678, \"clientId\": 1234,
\"ramaScore\": 68.55655, \"temporalScore\": {\"id\": null,
\"temporalScore\": 24.0, \"hnmScore\": 24.0, \"siemScore\": 0.0,
\"ramaScore\": null}, \"baseScore\": {\"id\": null, \"baseScore\": 34.6335,
\"hccScore\": 0.0, \"hetScore\": 4.95, \"vulnerabilityAssessmentScore\":
100.0, \"ramaScore\": null}, \"created\": \"2022-02-03 17:32:39\",
\"updated\": \"2022-02-03 17:32:39\", \"clientStatus\": \"Medium\",
\"metadata\": {\"hospitalId\": 5678, \"clientId\": 1234, \"host_name\":
\"BPRELIPCEAN-L2\", \"machine_id\":
\"3119BFD93119E3AB3119D0123119960B3119B2ED3119FDE63119DF543119C5BB3119FC353
11994B33119DB3C3119D9C23119A1363119BCC73119BDB63119F25A\",
\"hospital_region\": \"Hospital A from region B\", \"hospital_address\":
\"Street no 1\", \"connected_clients\": \"1\", \"hccMetadata\":
{\"numberOfIdentifiedHeartbleeds\": 0, \"identifiedHeartbleeds\": []},
\"hetMetadata\": {\"noOfOSVulnerabilities\": 1, \"noOfMisconfigurations\":
14, \"numberOfBenignFindings\": 11, \"numberOfMaliciousFindings\": 4,
\"percentageOfBenignFindings\": 73.33333333333333,
\"percentageOfMaliciousFindings\": 26.666666666666668, \"hetVector\":
```

```
\"C:L/I:L/A:N\"}, \"vulnerabilityAssessmentAggregatedMetadata\":
{\"vulnerabilityAssessmentMetadata\": [{\"application_name\": \"Mozilla
Firefox\", \"noOfVulnerabilities\": 55, \"vulnerabilities\": [\"CVE-2011-
0064\", \"CVE-2021-29980\", \"CVE-2021-29983\", \"CVE-2021-29961\", \"CVE-
2021-38496\", \"CVE-2021-29989\", \"CVE-2021-38493\", \"CVE-2021-23994\",
\"CVE-2021-23981\", \"CVE-2021-38500\", \"CVE-2021-23996\", \"CVE-2021-
38499\", \"CVE-2021-23998\", \"CVE-2021-38497\", \"CVE-2021-23983\", \"CVE-
2021-29991\", \"CVE-2021-29968\", \"CVE-2021-29988\", \"CVE-2021-38494\",
\"CVE-2021-23986\", \"CVE-2021-23985\", \"CVE-2021-29944\", \"CVE-2021-
23997\", \"CVE-2021-29947\", \"CVE-2021-29981\", \"CVE-2021-38492\", \"CVE-
2021-29984\", \"CVE-2021-29946\", \"CVE-2021-23988\", \"CVE-2021-38501\",
\"CVE-2015-4000\", \"CVE-2007-3670\", \"CVE-2021-23982\", \"CVE-2021-
23999\", \"CVE-2021-29955\", \"CVE-2021-24001\", \"CVE-2021-23995\", \"CVE-
2021-29982\", \"CVE-2021-29990\", \"CVE-2021-29960\", \"CVE-2021-23987\",
\"CVE-2021-29959\", \"CVE-2021-29987\", \"CVE-2021-29951\", \"CVE-2021-
29967\", \"CVE-2021-23984\", \"CVE-2021-29964\", \"CVE-2021-29985\", \"CVE-
2021-38491\", \"CVE-2021-24000\", \"CVE-2021-29966\", \"CVE-2021-38498\",
\"CVE-2021-29986\", \"CVE-2021-24002\", \"CVE-2011-3389\"]}],
\"top10Vulnerabilities\": {\"CVE-2011-0064\": 67, \"CVE-2021-29980\": 67,
\"CVE-2021-38496\": 67, \"CVE-2021-29989\": 67, \"CVE-2021-38493\": 67,
\"CVE-2021-23994\": 67, \"CVE-2021-38500\": 67, \"CVE-2021-38499\": 67,
\"CVE-2021-29988\": 67, \"CVE-2021-38494\": 67},
\"totalNoOfVulnerabilities\": 55}, \"hwcMetadata\": null, \"hnmMetadata\":
{\"hnmMetadata\": [{\"destinationPort\": 49671, \"destinationIp\":
\"10.18.139.78\", \"sourcePort\": 35168, \"sourceIp\": \"10.18.139.58\",
\"description\": \"Network probe has detected a request to a suspicious DNS
domain.\"}, {\"destinationPort\": 222, \"destinationIp\": \"10.18.139.78\",
\"sourcePort\": 35168, \"sourceIp\": \"10.18.139.58\", \"description\":
\"Network probe has detected a request to a suspicious DNS domain.\"},
{\"destinationPort\": 50975, \"destinationIp\": \"192.168.198.204\",
\"sourcePort\": 445, \"sourceIp\": \"192.168.198.203\", \"description\":
\"Network Probe has prevented a suspicious DNS request to a public server
that could contain private data. This is a potential data exfiltration
marker. Data exfiltration is a form of a security breach that occurs when
an individual's or company's data is copied, transferred, or retrieved from
a computer or server without authorization.\"}], \"totalHNMFindings\": 3,
\"numberOfAttacks\": 3, \"numberOfExploits\": 0}, \"indicators\": {\"id\":
0, \"hnmScore\": 24.0, \"hccScore\": 0.0, \"hetScore\": 4.95, \"vaScore\":
100.0, \"facilitatorScore\": 0.0, \"calculated\": null}, \"ramaVector\":
null, \"numberOfCriticalEvents\": 59}}, {\"hospitalId\": 5678,
\"clientId\": 1, \"ramaScore\": 68.55655, \"temporalScore\": {\"id\": null,
\"temporalScore\": 24.0, \"hnmScore\": 24.0, \"siemScore\": 0.0,
\"ramaScore\": null}, \"baseScore\": {\"id\": null, \"baseScore\": 34.6335,
\"hccScore\": 0.0, \"hetScore\": 4.95, \"vulnerabilityAssessmentScore\":
100.0, \"ramaScore\": null}, \"created\": \"2022-02-03 17:39:18\",
\"updated\": \"2022-02-04 11:43:25\", \"clientStatus\": \"Medium\",
\"metadata\": {\"hospitalId\": 5678, \"clientId\": 1, \"host_name\":
\"BPRELIPCEAN-L2\", \"machine_id\":
\"3119BFD93119E3AB3119D0123119960B3119B2ED3119FDE63119DF543119C5BB3119FC353
11994B33119DB3C3119D9C23119A1363119BCC73119BDB63119F25A\",
\"hospital_region\": \"Hospital A from region B\", \"hospital_address\":
\"Street no 1\", \"connected_clients\": \"1\", \"hccMetadata\":
{\"numberOfIdentifiedHeartbleeds\": 0, \"identifiedHeartbleeds\": []},
\"hetMetadata\": {\"noOfOSVulnerabilities\": 1, \"noOfMisconfigurations\":
14, \"numberOfBenignFindings\": 11, \"numberOfMaliciousFindings\": 4,
\"percentageOfBenignFindings\": 73.33333333333333,
\"percentageOfMaliciousFindings\": 26.666666666666668, \"hetVector\":
\"C:L/I:L/A:N\"}, \"vulnerabilityAssessmentAggregatedMetadata\":
{\"vulnerabilityAssessmentMetadata\": [{\"application_name\": \"Mozilla
Firefox\", \"noOfVulnerabilities\": 55, \"vulnerabilities\": [\"CVE-2021-
23984\", \"CVE-2021-29980\", \"CVE-2011-3389\", \"CVE-2021-29944\", \"CVE-
```

```
2021-29951\", \"CVE-2021-29981\", \"CVE-2021-23987\", \"CVE-2021-23981\",
\"CVE-2021-23998\", \"CVE-2021-29982\", \"CVE-2021-29961\", \"CVE-2021-
23983\", \"CVE-2021-38499\", \"CVE-2021-23994\", \"CVE-2021-38501\", \"CVE-
2021-38494\", \"CVE-2021-23982\", \"CVE-2021-38498\", \"CVE-2021-23997\",
\"CVE-2021-23985\", \"CVE-2021-29960\", \"CVE-2021-38497\", \"CVE-2021-
29967\", \"CVE-2021-29983\", \"CVE-2021-38491\", \"CVE-2007-3670\", \"CVE-
2021-29990\", \"CVE-2021-29988\", \"CVE-2021-29955\", \"CVE-2021-29966\",
\"CVE-2021-24001\", \"CVE-2021-24000\", \"CVE-2021-29991\", \"CVE-2021-
29985\", \"CVE-2021-24002\", \"CVE-2021-23999\", \"CVE-2021-29964\", \"CVE-
2021-29959\", \"CVE-2021-29986\", \"CVE-2021-38492\", \"CVE-2021-23995\",
\"CVE-2021-38496\", \"CVE-2021-23988\", \"CVE-2021-29968\", \"CVE-2015-
4000\", \"CVE-2011-0064\", \"CVE
```