D3.1

The HEIR 1st layer of services package for the MVP

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.	D3.1
Workpackage	WP3
Due date	08-2021-M12
Actual submission date	01/09/2021

Deliverable lead	STS
Editors	ZACHARAKIS A., LEVENTIS C., KOLOUTSOU K (STS)
Contributors	Gavrilut Dragos, Prelipcean Bogdan (BD), Iulia Ilie(SIE), Andreas Alexopoulos, Leonidas Kalipollitis (AEGIS)
Reviewers	George Tsakirakis (ITML), SIE
Dissemination level	PU
Revision	1.0
Keywords	MVP prototype

Abstract

This deliverable serves as an accompanying report which refers to the release of the MVP of HEIR. The described work emphasizes the development of the envisioned MVP integrated HEIR prototype, ensuring a smooth and effective integration of the components that compose this proof of concept demonstrator.

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 Minimum Viable Product - MVP. The development of the MVP demonstrates the effective integration of the 1st layer components into a simple, yet substantially integrated prototype with minimum functionality that showcases the potential of the proposed solution.

The 1st layer of services package for the MVP 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. The MVP will serve as the basis for further developments and will drive the implementation toward the release of complete prototypes (M18-M30). MVP release will act as proof of concept demonstrator.

The deliverable is organized into five sections whose purpose is briefly described next.

Section 1 introduces the deliverable, Section 2 presents the MVP definition, the MVP development, and the subsequent steps towards the establishment of fully functional prototypes, Section 3 describes the HEIR MVP architecture and provides deployment details of the MVP infrastructure. The section also describes the integration actions and the communication mechanism used to connect the components. Section 4 presents the use case scenarios. Section 5 highlights the overall conclusions and plans.

Table of Contents

LIST OF ABBREVIATIONS

HCC HEIR Cryptographic Checker

HCG HEIR Client GUI

HET HEIR Exploit Tester

HNM HEIR Network Module

MVP Minimum Viable Product

RAMA Risk Assessment for Medical Applications

LIST OF FIGURES

1. Introduction

1.1 Scope and objectives

The document aims to present the development of HEIR's 1st layer of services package for the MVP, a prototype with minimum functionality that showcases the potential of the proposed solution and forms the basis for further developments towards the release of the first and final versions of the HEIR integrated prototypes.

1.2 Relation to other Tasks and Work Packages

This document is related to all the Tasks and deliverables of WP3. Moreover, there is a close interrelation between this deliverable and the WP4 and WP5 deliverables.

More specifically, this deliverable is strongly connected to (a) "D4.1 - The HEIR 2nd layer of services package for the MVP", as the 2nd layer contains the HEIR global benchmark against which the RAMA scores of medical infrastructures will be compared and, (b) to "D5.2 - HEIR Minimum Viable Product" as HEIR 1st layer of services packaging will be part of the overall HEIR MVP.

2. MVP definition

2.1 Methodology

MVP stands for Minimum Viable Product, and it is a version of the product where only the main features are completed. The purpose of the MVP is to present the basic components to early customers or end-users so that, with minimal effort, the development teams can collect the maximum amount of feedback. In addition, an MVP plays the role of ensuring that the features of the project are feasible and are ready for testing by the end-users. The feedback provided by the users can give insights regarding the customer's interests and is used as a guide by the developers for corrections, future developments, and improvements.

2.2 HEIR 1st layer of services MVP

The HEIR 1st layer of services MVP includes the basic functional components of the HEIR system. It is based on specific predefined pilot scenarios to showcase the abilities of the overall system and ensure the functionalities of the proposed components.

Unfortunately, the ongoing Covid-19 situation affected the development process, and some components did not meet the initial expectations. That being said, the full MVP 1st layer of services package will be integrated into PAGNI's local environment whereas individual components of the package (such as the Threat Detection Module) will be deployed in the rest of the use case providers.

For the HEIR 1st layer of services MVP, data is mainly collecting from the HEIR Exploit Tester and the Vulnerability Assessment Module.

Operational System and application vulnerabilities are collected through the HEIR Exploit tester and the vulnerability assessment modules respectively. Following this, the HEIR Client, a multi-modular application, aggregates the results and feeds them to the Risk Assessment for Medical Applications (RAMA) calculator. The latter then continuously calculates the RAMA score that depicts the security status of the hospital.

The results are then forwarded to the HEIR Aggregator and the HEIR Client GUI.

3. 1st layer of services MVP architecture

3.1 Overview

This subsection presents an overview of the 1st layer of services package MVP Architecture. Figure 1 illustrates a high-level overview of the MVP architecture and the different components within the 1st layer. More specifically, the components are (a) the Novel HEIR Client, (b) the Threat Hunting Module, (c) the RAMA Score Calculator, (d) the HEIR Client GUI and (e) the novel HEIR Aggregator.

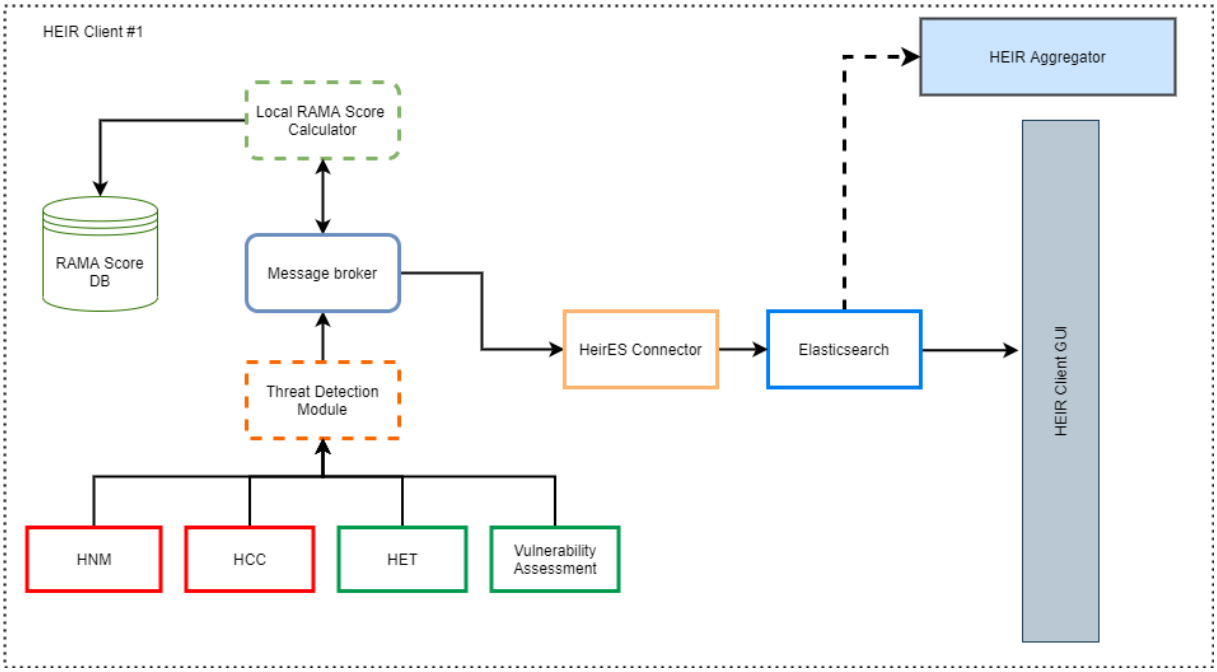

Figure 1 1st layer of services MVP Architecture

3.2 Novel HEIR Client

The novel HEIR Client collects and processes information, either on the endpoint level or a centralized one. The architecture of the HEIR client is modular allowing to plugin several analysis components (HEIR Network Module, HEIR Cryptographic Checker, HEIR Exploit Tester, and Vulnerability Assessment). For the MVP, the HEIR Exploit Tester and Vulnerability assessment modules are being used.

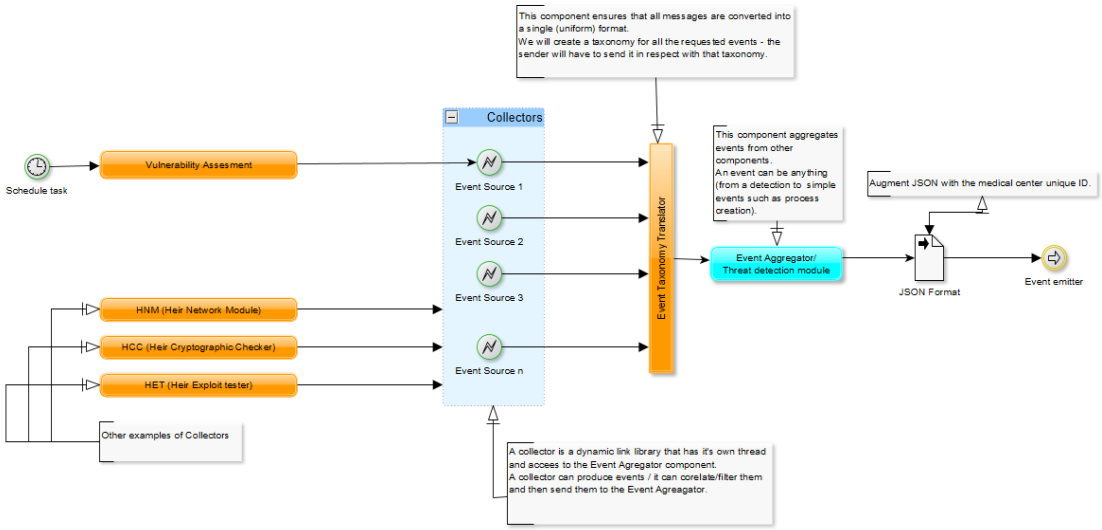

Figure 2 HEIR Client Architecture

The Collectors send events with information about threats, security metrics, and risk. The events are normalized and converted to a single and uniform format by the Event Taxonomy Translator component. The normalized events are then aggregated by the Event Aggregator component. This compone also correlates and augments the events and then provides them to the RAMA score calculator. The events are submitted to the RAMA Score Calculator through the HEIR's Kafka Message Broker.

For the MVP, the provided modules are the HEIR Exploit Tester (HET) and the Vulnerability Assessment module which provides information about:

- system misconfiguration on the endpoint system
- application vulnerability assessment

The output of the module that is integrated into the HEIR client and is further provided to the RAMA score calculator is shown in Appendix B – Nover HEIR Client sample output.

3.3 Threat detection module

The threat detection module is a module that can centralize and correlate the information regarding threats from the other components e.g., the threat detection components from the facilitators or the HEIR Exploit Tester module. The architecture of the module is similar to the internal architecture of the HEIR client with the focus on the Event Aggregator and Augmentation component:

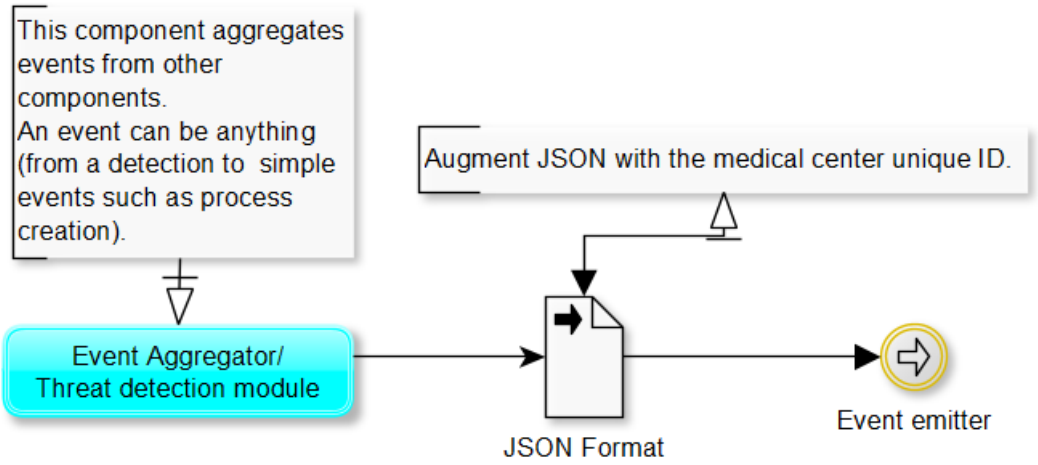

Figure 3 Threat Detection Module – High-level architecture

The events are being continuously submitted to the RAMA Score Calculator through HEIR's Kafka Message Broker.

3.4 The Local RAMA Score calculator

The RAMA score acts as a benchmark for the IT security of a hospital or healthcare facility. It is responsible for estimating the attack surface and resilience of the medical devices by incorporating several critical issues in a live manner. To calculate the score, the RAMA Score Calculator receives aggregated input from several HEIR components, through the HEIR Client. These components are:

a) the HEIR Network Module (HNM)
b) the HEIR Exploit Tester (HET)
c) the HEIR Cryptographic Checker (HCC)
d) the Vulnerability Assessment module and,

Two types of scores can be identified, the local and the global. The local RAMA score represents the security level of a specific sector clinic by aggregating the respective results whereas the global RAMA score acts as an aggregator of all the local scores of a healthcare facility and provides a unified score. This allows to conceal information about specific vulnerable sectors but reflects the aggregated result. The latter will be described in "D4.1 - The HEIR 2nd layer of services package for the MVP"

For the MVP, the local RAMA Score calculator will receive input from the (b) and (e). To do so, RAMA Score Calculator subscribes to the "HeirClientToRama" Kafka topic, which includes the aggregated events of the above-mentioned components, as provided by the HEIR Client.

Then, the RAMA score is being computed based on the following algorithm:

Base equation :

- case DecreasedRAMAScore:
  - case 0
    - Do nothing
  - else

        - (HNSScore) /20 – (HWCScore) /20 – (HETScore) /20 – (VulnAssessmentScore) /20 – (HCCScore) /20 – (ResilienceScore) /20
- case IncreasedRAMAScore:
    - case 100
        - Do nothing
    - else
        - (HNSScore)/20 + (HWCScore) /20 + (HETScore) /20 + (VulnAssessmentScore) /20 + (HCCScore) /20 + (ResilienceScore) /20

where:

- **HNSScore** = (Number of Unknown or non-preauthorized devices) * 2.5
- **HWSScore** = (Number of not pre-approved devices) * 2.5 + (Number of not pre-approved software applications) *2.5 + (Number of not pre-approved network access-points) * 2.5
- **VulnAssessmentScore** = (Number of matchedVulnerabilities) * 2
- **HCCScore** = (Number of devices/web services with obsolete cyphers) * 0.5
- **ResilienceScore** = (Number of components that failed the stress test) * 2
- **HETScore**: case matchedVulnerabilitiesToExploits (Triggered=TRUE):
    - (0.85* ((Impact*Confidentiality)+ (Impact * Availability) + (Impact * Integrity)) + (0.15*((Impact*Confidentiality)+ (Impact * Availability) + (Impact * Integrity)))
        - Impact
        - none: 0.0
        - low : 2.0
        - medium: 7.0
        - high: 10.0

Finally, the computed RAMA score – alongside metadata received through the HEIR client- is being continuously provided, through the Kafka message broker, to the HeirES connect. The latter is responsible to store the above-mentioned information to elasticsearch so that it can be made available to the HEIR Client's GUI and the HEIR Aggregator.

The RAMA Score calculator's output is available in Figure 4.

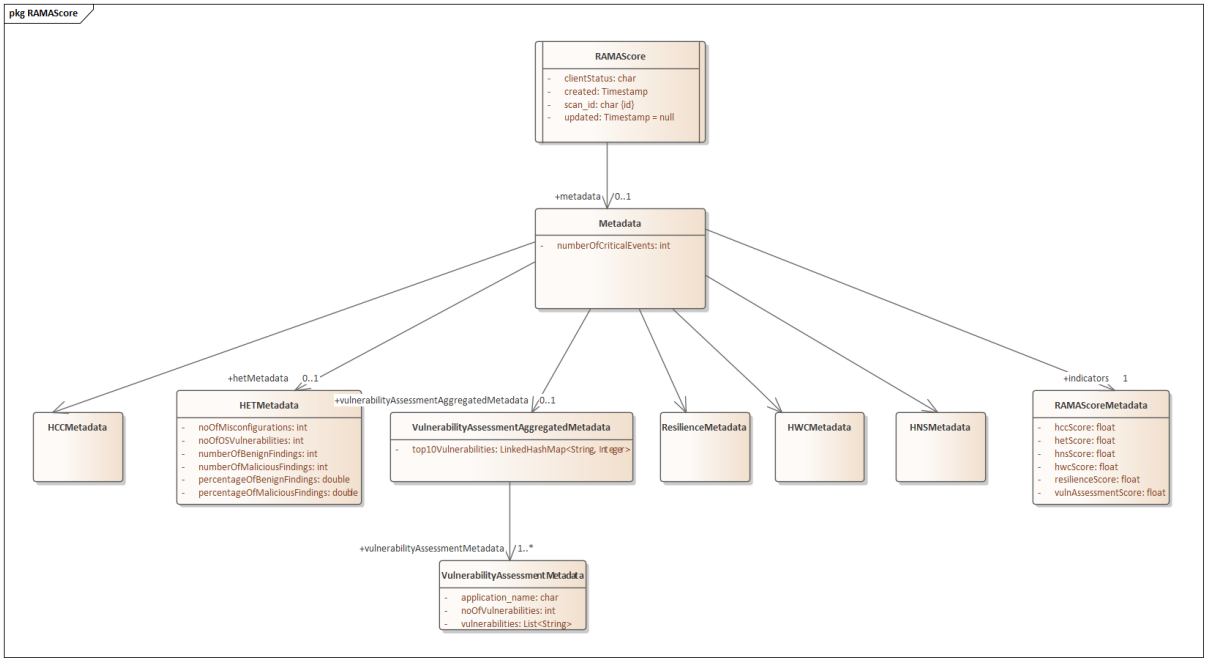

Figure 4 RAMA Score Calculator Output (UML)

A sample output of the RAMA Score calculator is available in Appendix A – RAMA Score Calculator sample output.

3.5 HEIR Client GUI

The HEIR Client GUI (HCG) includes visualizations of information generated by the 1st level services running inside a hospital environment. This information will be only available to authorized users belonging to the hospital staff since it will contain 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 RAMA score and the global one, thus providing users with an idea of how their hospital stands with regards to other similar infrastructures.

In the context of MVP, users accessing the HCG will view the RAMA score of the HEIR Client deployed in PAGNI as calculated by the threat detection module and the score calculator described in the previous paragraphs. This is directly compared with the global RAMA score coming from the Observatory. Both of the scores comprise the upper level of the HCG's page as seen in Figure 5 below.

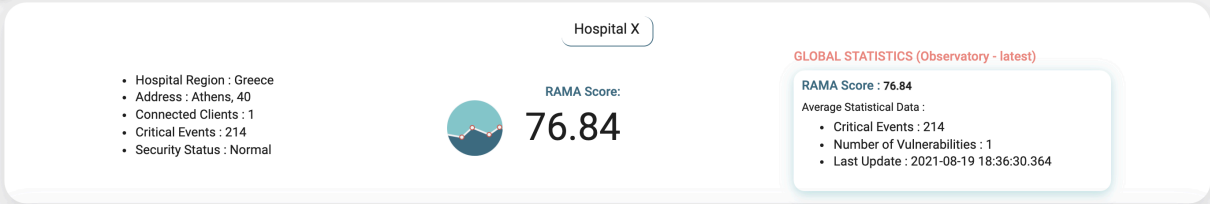

Figure 5 HCG: Local and Global RAMA scores

Following the components contributing to the RAMA score calculation, each specific subscore together with a brief description of what it represents is available to users. These are displayed in the following section of the page together with an overview of the historical evolution of the RAMA score for a user-defined time period defaulting at the most recent week. Figure 6 below depicts how this information is presented.

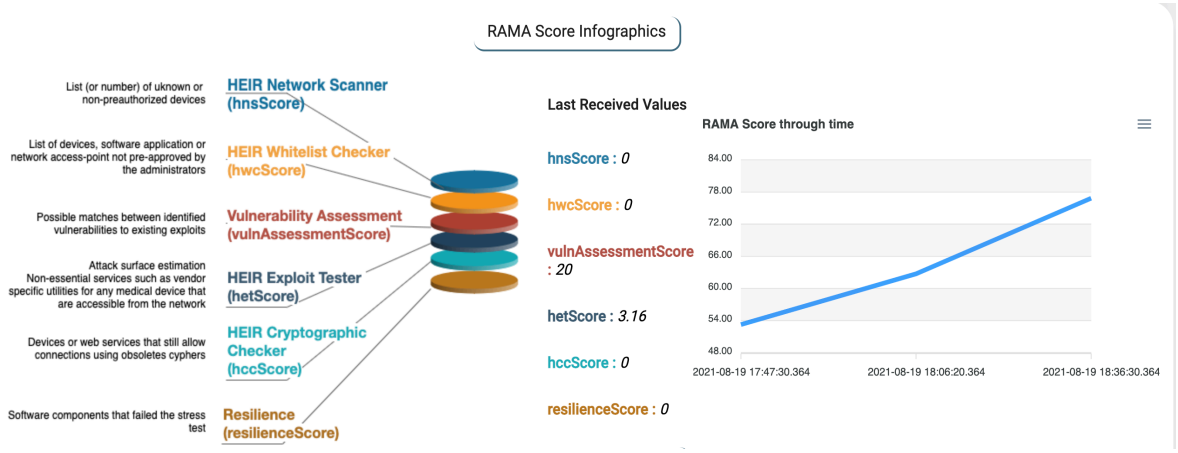

Figure 6 HCG: RAMA sub-scores and Historical RAMA Score evolution

The last part of the page displays the connected HEIR Clients of the inspected hospital. For MVP purposes only one client is deployed, therefore statistics on total detected vulnerabilities, captured events, and applications vulnerabilities stem from this client (Figure 7). Specifically, vulnerabilities found in various applications can be further expanded and users can get the exact vulnerabilities detected per application so that they know exactly what is affecting the produced

RAMA Score. It is foreseen that as soon as more than one client is deployed in a hospital, the displayed numbers will be populated by the rest of the clients' data and aggregated statistics will be presented to users. At the lowest part of this section, users also can click on the 'Inspect' button of a client and open up the Forensics Visualisation Toolkit (FVT) which presents the captured events in a more detailed way as described in D2.1.

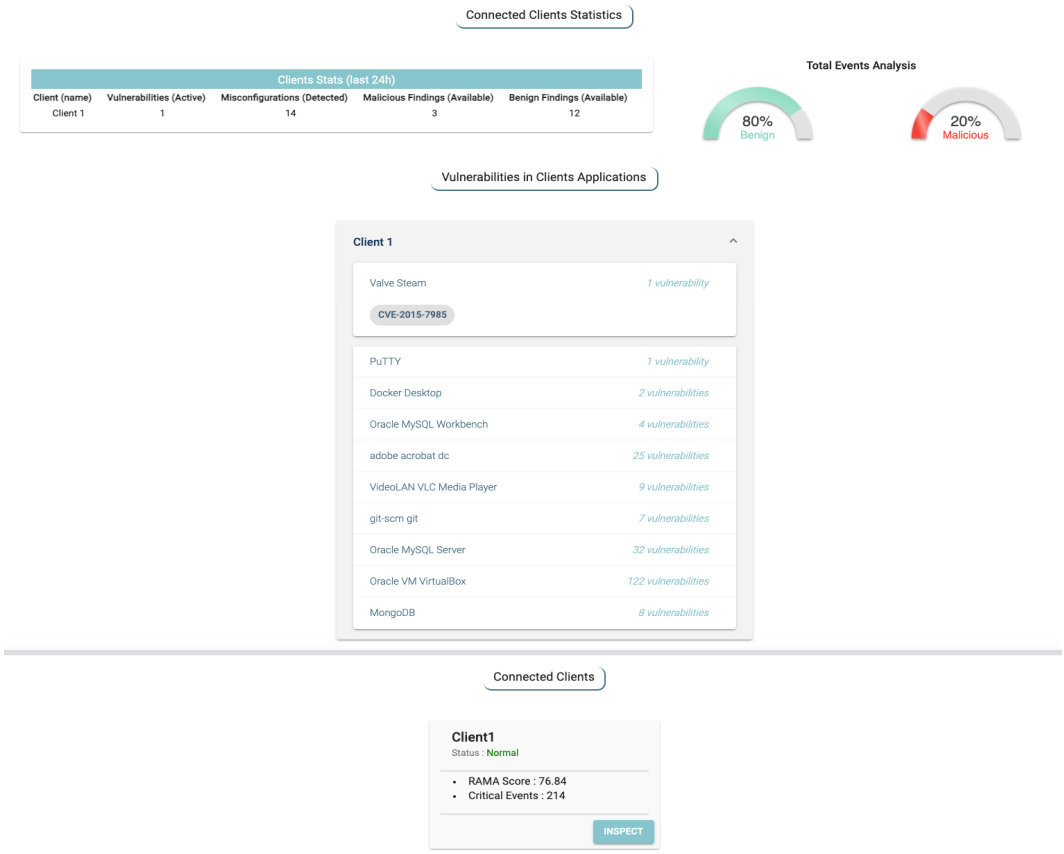

Figure 7 HCG: Client Statistics

The visualization elements described in the previous paragraphs form the HCG version for the MVP. This is the starting point for building up the functionality needed to cover the needs of all the pilots in view of the upcoming integrated version of the HEIR platform in M18. The complete HCG page is presented in Figure 8 below.

Figure 8 HCG: Complete page for MVP

3.6 The novel HEIR Aggregator

The HEIR Aggregator is a component of the HEIR framework designed for health institutions with multiple independent departments.

The Aggregator compiles statistical information on possible events or vulnerabilities discovered by the HEIR clients for the independent departments. An aggregated local RAMA score is also computed after having been provided with multiple local RAMA scores by the HEIR clients deployed on the individual departments.

For the current MVP demonstrated on the PAGNI environment, there is only one HEIR client for which to compute the aggregates. Nevertheless, once there are multiple HEIR clients independently writing to the Elasticsearch storage from one institution, the HEIR Aggregator is capable of compiling both the Rama scores and the statistical information on HEIR client status.

The HEIR Aggregator will be triggered based on a user-defined schedule (e.g. hourly), read the most recent outputs from the HEIR clients from the Elasticsearch storage, compute the aggregates, and write the aggregated values for RAMA and event statistics to the Elasticsearch storage, where they can be accessed by the HEIR GUI. In the following iterations of the MVP, the Aggregator will also send its output to the HEIR Observatory database.

The aggregation flow is illustrated below in Figure 9.

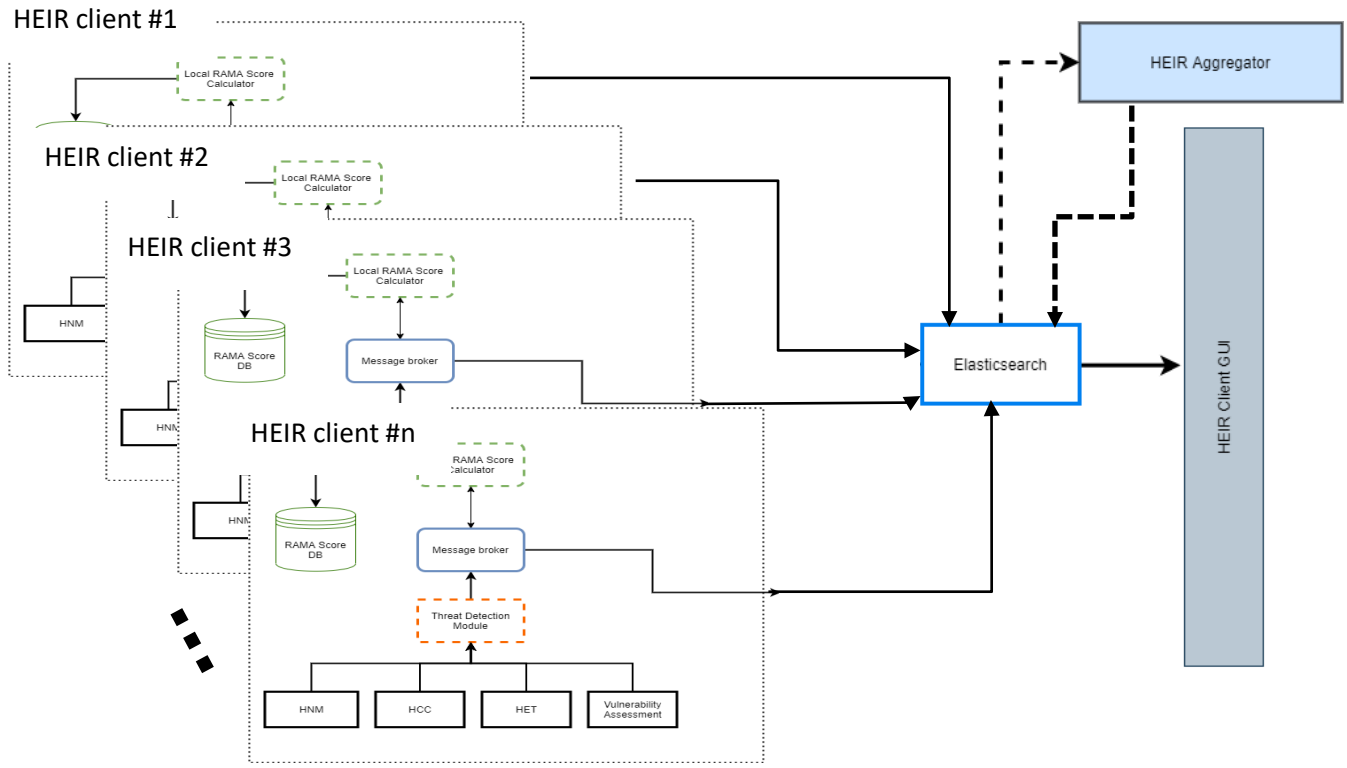

Figure 9. HEIR Aggregator

4. 1st layer of services package MVP use case scenario

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 hospitalization 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 MVP, we will deploy the 1st layer of services package in PAGNI's local environment to identify potential issues. The Local RAMA Score will be calculated based on these findings.

The flow of the MVP scenarios is as follows:

- The Endpoint component for Risk Analytics is deployed into the endpoints from the hospital infrastructure
- A scheduled task will run the Risk Analytics tool that will generate an event (report) regarding misconfiguration risks and application vulnerability assessment.
- The generated event will be normalized and aggregated by the HEIR Client (at the endpoint level in this point) and then emitted to the message broker (Kafka)
- 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.

The module communication for the above described used case is depicted in Figure 10.

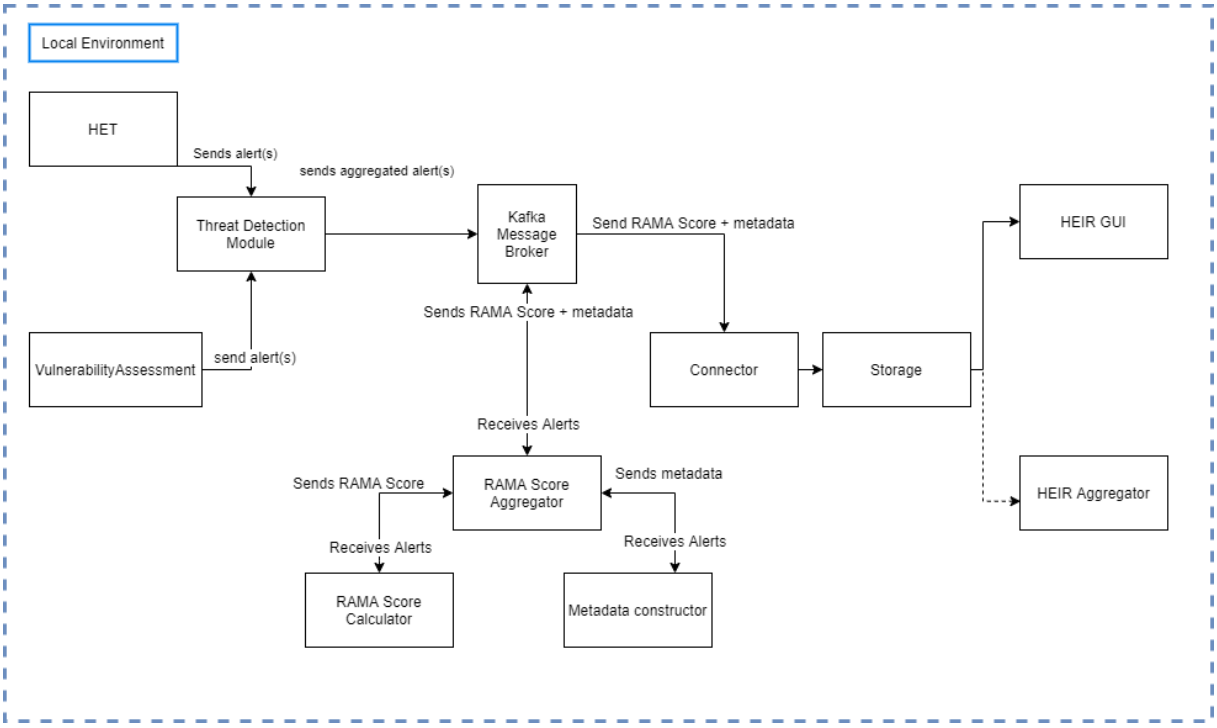

Figure 10 Modules communication

5. Conclusion

The current deliverable describes the implementation and rationale behind the HEIR 1st Layer of services MVP. It analyses the MVP use case scenarios and explains how and why they were selected. The main objective of these use cases is to validate and test the HEIR 1st layer of services architecture and to initiate the integration between the 1st layer's components. For each component, the work performed to support the operation of the MVP is being described. Lastly, we also present the communication methods and the integration elements that enabled the delivery of the MVP, based on the proposed use cases.

The next steps will be concentrated on the completion of HEIR's 1st layer of services package. This will be based on the progress of the technical work packages, as well as the feedback to be obtained from the MVP. The 1st completed version will be reported in D3.2 - "The HEIR 1st layer of services package: 1st complete version".

6. Appendix A – RAMA Score Calculator sample output


```
{
    "score": 56.164997,
    "metadata": {
        "hospital_region": "Hospital A from region B",
        "vulnerabilityAssessmentAggregatedMetadata": {
            "vulnerabilityAssessmentMetadata": [
                {
                    "application_name": "Mozilla Firefox",
                    "noOfVulnerabilities": 44,
                    "vulnerabilities": [
                        "CVE-2021-23981",
                        "CVE-2021-29987",
                        "CVE-2011-0064",
                        "CVE-2021-29986",
                        "CVE-2021-29968",
                        "CVE-2021-23994",
                        "CVE-2021-23988",
                        "CVE-2021-23985",
                        "CVE-2021-29964",
                        "CVE-2021-23996",
                        "CVE-2021-24000",
                        "CVE-2021-23983",
                        "CVE-2021-29946",
                        "CVE-2021-29981",
                        "CVE-2021-29955",
                        "CVE-2021-29985",
                        "CVE-2021-24002",
                        "CVE-2021-29951",
                        "CVE-2021-29983",
                        "CVE-2011-3389",
                        "CVE-2021-29990",
                        "CVE-2021-23987",
                        "CVE-2021-29959",
                        "CVE-2021-23984",
                        "CVE-2021-29947",
                        "CVE-2021-29988",
                        "CVE-2021-29980",
                        "CVE-2007-3670",
                        "CVE-2015-4000",
                        "CVE-2021-29967",
                        "CVE-2021-29961",
                        "CVE-2021-23998",
                        "CVE-2021-24001",
                        "CVE-2021-23999",
                        "CVE-2021-23997",
                        "CVE-2021-29984",
                        "CVE-2021-23986",
                        "CVE-2021-29982",
                        "CVE-2021-29960",
                        "CVE-2021-23982",
                        "CVE-2021-23995",
                        "CVE-2021-29966",
                        "CVE-2021-29944",
                        "CVE-2021-29989"
                    ]
                }
            ],
            "totalNoOfVulnerabilities": 44,
            "top10Vulnerabilities": {
```

```
                "CVE-2021-23987": 67,
                "CVE-2021-23988": 67,
                "CVE-2021-29981": 67,
                "CVE-2021-29990": 67,
                "CVE-2011-0064": 67,
                "CVE-2021-29986": 67,
                "CVE-2021-29985": 67,
                "CVE-2021-24002": 67,
                "CVE-2021-29946": 67,
                "CVE-2021-23994": 67
            }
        },
        "numberOfCriticalEvents": 46,
        "connected_clients": "1",
        "machine_id":
"6648CB546648B67E6648EC0E6648B0C26648FB106648C7336648EE946648DB6C6648B51566
48E8426648E43C6648DEDD66488046664885B26648B4656648F0F8",
        "hetMetadata": {
            "numberOfMaliciousFindings": 2,
            "percentageOfBenignFindings": 86.66666666666667,
            "noOfOSVulnerabilities": 1,
            "percentageOfMaliciousFindings": 13.333333333333334,
            "noOfMisconfigurations": 14,
            "numberOfBenignFindings": 13
        },
        "indicators": {
            "hnsScore": 0,
            "hwcScore": 0,
            "vulnAssessmentScore": 44,
            "hetScore": 0.825,
            "hccScore": 0,
            "id": 0,
            "resilienceScore": 0
        },
        "hospital_address": "Street no 1",
        "host_name": "HEIR-WIN10"
    },
    "created": "2021-08-26 13:35:51.668",
    "clientStatus": "Critical",
    "scan_id": "c74a2b58-2fa6-408e-b40d-152fd35ea66b",
    "updated": "2021-08-30 20:15:04.642"
}
```

7. Appendix B – Nover HEIR Client sample output

{
"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": true,
"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": true,
"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": "High",

"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": true,

"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": true,

"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 <driveletter> on <computername>. 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": false,
        "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"
    }
],
"host_name": "DESKTOP-7KHP3O2",
```

```
"host_os": "Windows 10",
"scan_id": "c74a2b58-2fa6-408e-b40d-152fd35ea66b",
"scan_status": "finished",
"machine_id": "32",
"hospital_region": "PAGNI",
"hospital_address": "Panepistimiou, Iraklio 715 00",
"connected_clients": 1,
"vulnerabilityAssessment": [
  {
    "application_name": "Docker Desktop",
    "cves": [
      {
        "cve": "CVE-2018-10892",
        "description": "The default OCI linux spec in oci/defaults{_linux}.go in Docker/Moby from 1.11 to current does not block /proc/acpi pathnames. The flaw allows an attacker to modify host's hardware like enabling/disabling bluetooth or turning up/down keyboard brightness.",
        "publish_date": "2018-07-06T16:29Z",
        "score": 50
      },
      {
        "cve": "CVE-2020-11492",
        "description": "An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.",
        "publish_date": "2020-06-05T14:15Z",
        "score": 72
      }
    ],
    "version": "2.2.0.4"
  },
  {
    "application_name": "git-scm git",
    "cves": [
      {
        "cve": "CVE-2019-1387",
```

"description": "An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. Recursive clones are currently affected by a vulnerability that is caused by too-lax validation of submodule names, allowing very targeted attacks via remote code execution in recursive clones.",

"publish_date": "2019-12-18T21:15Z",

"score": 67

},

{

"cve": "CVE-2019-1353",

"description": "An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. When running Git in the Windows Subsystem for Linux (also known as \\\\\\\\\\\\\\\\"WSL\\\\\\\\\\\\\\\\") while accessing a working directory on a regular Windows drive, none of the NTFS protections were active.",

"publish_date": "2020-01-24T22:15Z",

"score": 75

},

{

"cve": "CVE-2019-1348",

"description": "An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. The --export-marks option of git fast-import is exposed also via the in-stream command feature export-marks=... and it allows overwriting arbitrary paths.",

"publish_date": "2020-01-24T22:15Z",

"score": 36

},

{

"cve": "CVE-2019-19604",

"description": "Arbitrary command execution is possible in Git before 2.20.2, 2.21.x before 2.21.1, 2.22.x before 2.22.2, 2.23.x before 2.23.1, and 2.24.x before 2.24.1 because a \\\\\\\\\\\\\\\\"git submodule update\\\\\\\\\\\\\\\\" operation can run commands found in the .gitmodules file of a malicious repository.",

"publish_date": "2019-12-11T00:15Z",

"score": 93

},

{

"cve": "CVE-2020-11008",

"description": "Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. This bug is similar to CVE-2020-5260(GHSA-qm7j-c969-7j4q). The fix for that bug still left the door open for an exploit where _some_ credential is leaked (but the attacker cannot control which one). Git uses

external \\\\\\\\\\\\\\\"credential helper\\\\\\\\\\\\\\\" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that are considered illegal as of the recently published Git versions can cause Git to send a \\\\\\\\\\\\\\\"blank\\\\\\\\\\\\\\\" pattern to helpers, missing hostname and protocol fields. Many helpers will interpret this as matching _any_ URL, and will return some unspecified stored password, leaking the password to an attacker's server. The vulnerability can be triggered by feeding a malicious URL to `git clone`. However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The root of the problem is in Git itself, which should not be feeding blank input to helpers. However, the ability to exploit the vulnerability in practice depends on which helpers are in use. Credential helpers which are known to trigger the vulnerability: - Git's \\\\\\\\\\\\\\\"store\\\\\\\\\\\\\\\" helper - Git's \\\\\\\\\\\\\\\"cache\\\\\\\\\\\\\\\" helper - the \\\\\\\\\\\\\\\"osxkeychain\\\\\\\\\\\\\\\" helper that ships in Git's \\\\\\\\\\\\\\\"contrib\\\\\\\\\\\\\\\" directory Credential helpers which are known to be safe even with vulnerable versions of Git: - Git Credential Manager for Windows Any helper not in this list should be assumed to trigger the vulnerability.",

"publish_date": "2020-04-21T19:15Z",

"score": 50

},

{

"cve": "CVE-2020-5260",

"description": "Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. Git uses external \\\\\\\\\\\\\\\"credential helper\\\\\\\\\\\\\\\" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that contain an encoded newline can inject unintended values into the credential helper protocol stream, causing the credential helper to retrieve the password for one server (e.g., good.example.com) for an HTTP request being made to another server (e.g., evil.example.com), resulting in credentials for the former being sent to the latter. There are no restrictions on the relationship between the two, meaning that an attacker can craft a URL that will present stored credentials for any host to a host of their choosing. The vulnerability can be triggered by feeding a malicious URL to git clone. However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The problem has been patched in the versions published on April 14th, 2020, going back to v2.17.x. Anyone wishing to backport the change further can do so by applying commit 9a6bbee (the full release includes extra checks for git fsck, but that commit is sufficient to protect clients against the vulnerability). The patched versions are: 2.17.4, 2.18.3, 2.19.4, 2.20.3, 2.21.2, 2.22.3, 2.23.2, 2.24.2, 2.25.3, 2.26.1.",

"publish_date": "2020-04-14T23:15Z",

"score": 50

},

{

"cve": "CVE-2021-21300",

"description": "Git is an open-source distributed revision control system. In affected versions of Git a specially crafted repository that contains symbolic links as well as files using a clean/smudge filter such as Git LFS, may cause just-checked out script to be executed while cloning onto a case-insensitive file system such as NTFS, HFS+ or APFS (i.e. the default file systems on Windows and macOS). Note that clean/smudge filters have to be configured for that. Git for Windows configures Git LFS by default, and is therefore vulnerable. The problem has been patched in the versions published on Tuesday, March 9th, 2021. As a workaound, if symbolic link support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. Likewise, if no clean/smudge filters such as Git LFS are configured globally (i.e. _before_ cloning), the attack is foiled. As always, it is best to avoid cloning repositories from untrusted sources. The earliest impacted version is 2.14.2. The fix versions are: 2.30.1, 2.29.3, 2.28.1, 2.27.1, 2.26.3, 2.25.5, 2.24.4, 2.23.4, 2.22.5, 2.21.4, 2.20.5, 2.19.6, 2.18.5, 2.17.62.17.6.",

"publish_date": "2021-03-09T20:15Z",

"score": 50

}

],

"version": "2.21.0"

}

]

}