Vulnerability Assessment as a Service - User Manual

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Table of contents

Table of figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

The Vulnerability Assessment as a Service (VAaaS) component of the SPHINX ecosystem discovers all existing and newly introduced network entities, assesses them against certain vulnerabilities and produces a Common Vulnerability Scoring System (CVSS) score that reflects the level of security of that particular entity. The vulnerabilities reports are then propagated to the Kafka service for all relevant components to retrieve. Moreover, the VAaaS component exposes a RESTful API to allow requests for ad-hoc assessments.

2 Installation/Deployment

2.1 Prerequisites and hardware

Minimum Requirements

- CPU: 2Cores
- RAM: 2GB
- GPU: Not needed
- SPACE: 3GB

2.2 Deployment with Docker

The VAaaS can be deployed on docker-compose. The deployment YAML is provided in the component's GIT repository.

2.3 Deployment with Kubernetes

The VAaaS can be deployed on K8S. The deployment YAML is provided in the component's GIT repository.

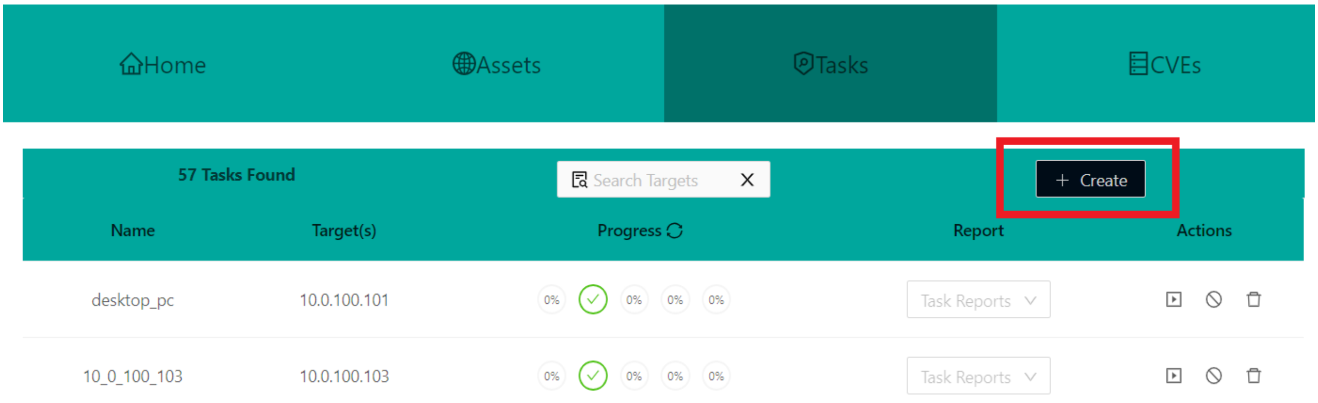
3 Operation and Maintenance

The basic example depicts the steps in order to assess an already existing network-enabled entity for vulnerabilities and retrieve the results of the assessment.

3.1 Basic Examples

For the **basic example,** navigate to the **"Tasks**" tab from the UI horizontal menu. A list of past assessments is displayed, should they exist, wherein the user can download the reports from the **"Report"** column, and restart/stop/delete the assessment from the **"Actions"** column bar. For the test case, select the "**Create"** button, which is located on the top right of the component (**Error! Reference source not found.**).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

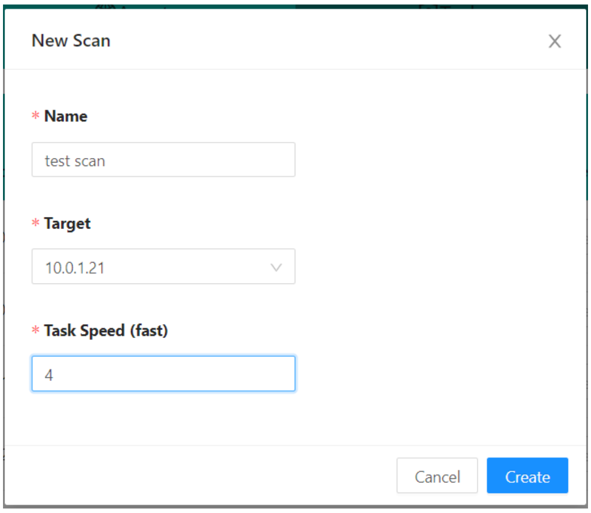


57 Tasks Found

Name	Target(s)	Progress	Report	Actions
desktop_pc	10.0.100.101	0% ✓ 0% 0% 0%	Task Reports	
10_0_100_103	10.0.100.103	0% ✓ 0% 0% 0%	Task Reports	

Figure 1 Select the "Create Button"

A modal, titled **"New Scan"** appears on the screen (Figure 3). Users are requested to fill in the task name ("**Name**"), target IP ("**Target**"), and assessment speed ("**Task Speed", from 1-5).** All three form elements are required for the assessment to start. Only when all three fields are filled, the **"Create"** button becomes enabled. Upon clicking the **"Create"** button the modal disappears, and the new task appears into the list (Figure 2).


New Scan

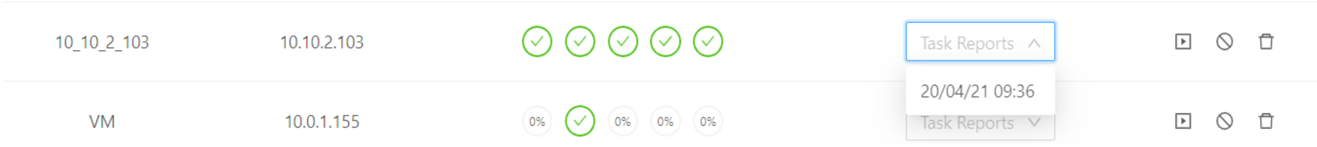
* Name: test scan

* Target: 10.0.1.21

* Task Speed (fast): 4

Figure 2 Create New Scan Modal

In the **"Progress"** column, 5 progress circles appear, each represents a unique sub-task of the assessment process. In the **"Progress"** column header there is a refresh button, which refreshes the progress of the sub-tasks. Upon completion of the assessment, the users can select the latest report by clicking the dropdown found in the **"Report"** column. By clicking the report, the detailed assessment is presented to the user along with the **"Save PDF"** button, wherein when clicked a pdf file containing the report results, is downloaded (Figure 3).



10_10_2_103	10.10.2.103	✓ ✓ ✓ ✓ ✓	Task Reports 20/04/21 09:36	
VM	10.0.1.155	0% ✓ 0% 0% 0%	Task Reports	

Figure 3 Download report

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3.2 Links with other Components

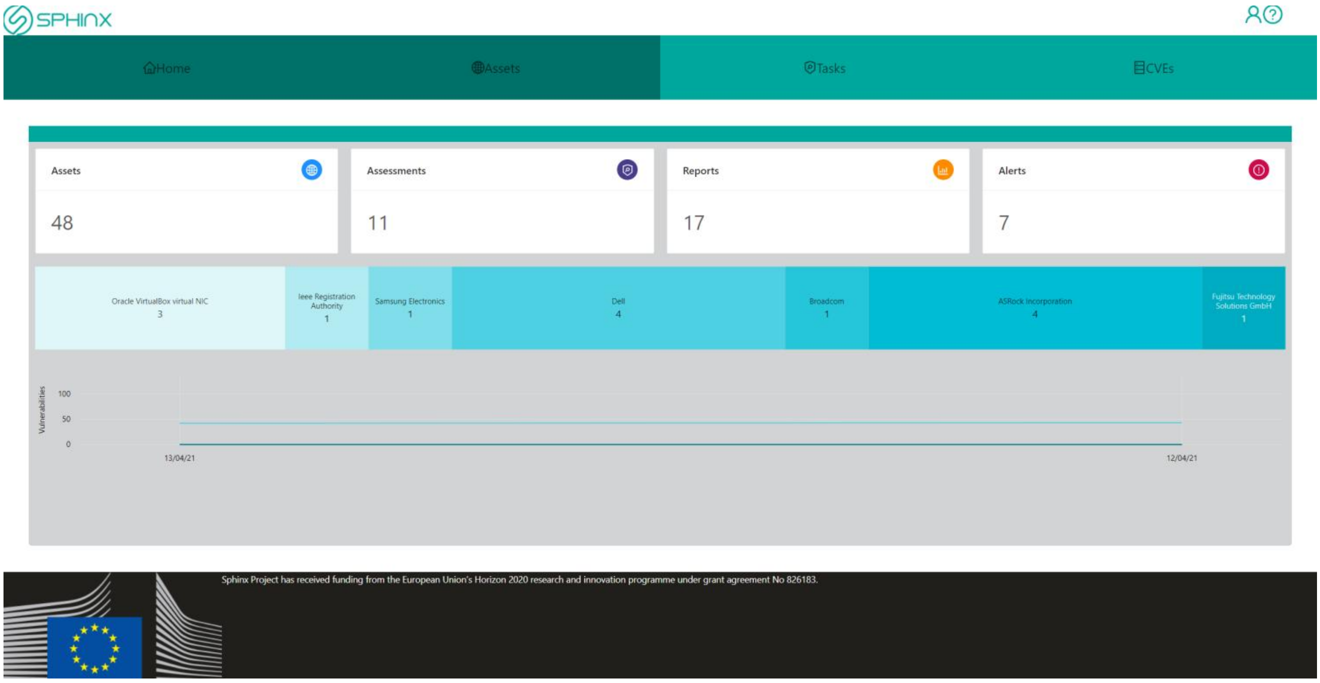
The VAaaS component is linked with the Kafka message broker service, through which all relevant components (e.g., Sandbox, Real-Time Cyber Risk Assessment (RCRA), etc.) can retrieve the latest VAaaS reports.

3.3 Outcomes

Upon finishing the assessment procedure, the users are presented with a detailed report containing the detected vulnerabilities of the selected network-enabled entity.

4 Application UI presentation

Figure 4 depicts the Home tab of the VAaaS dashboard, wherein the user can see various information of the infrastructure, such as the number of assets discovered in the network, the number of assessments, the number of existing vulnerability assessment reports, the number of entities that scored more than 5 in their CVSS scoring (named alerts), the detected system vendors, and the number of vulnerabilities per host.



Assets 48

Assessments 11

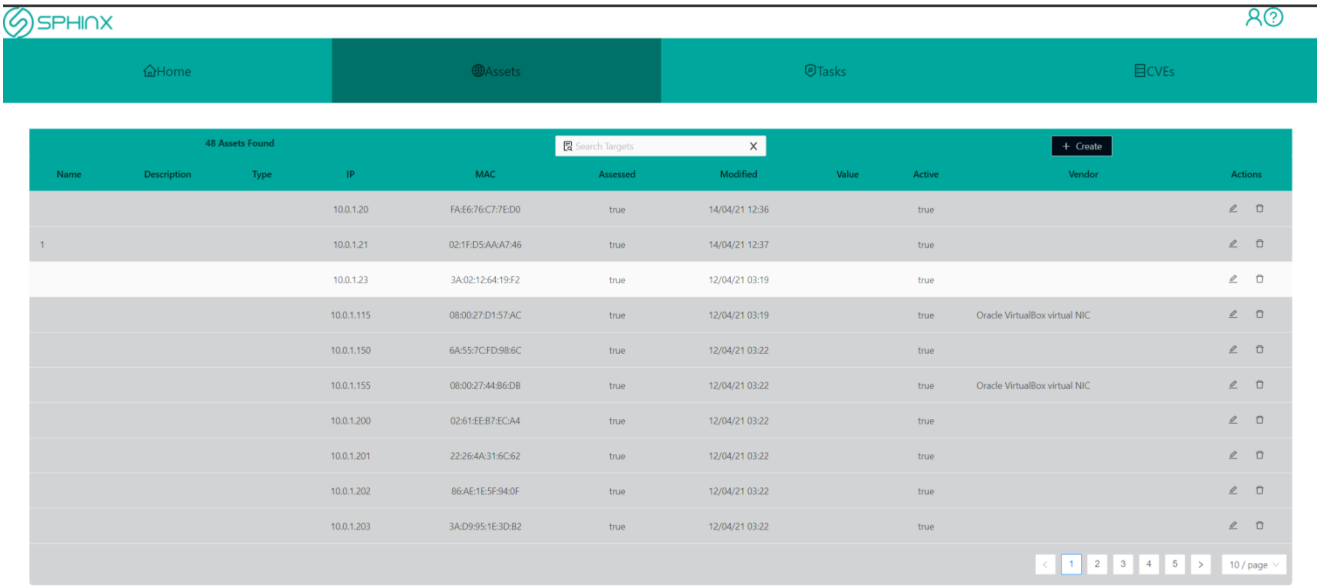
Reports 17

Alerts 7

Sphinx Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183.

Figure 4 Home tab

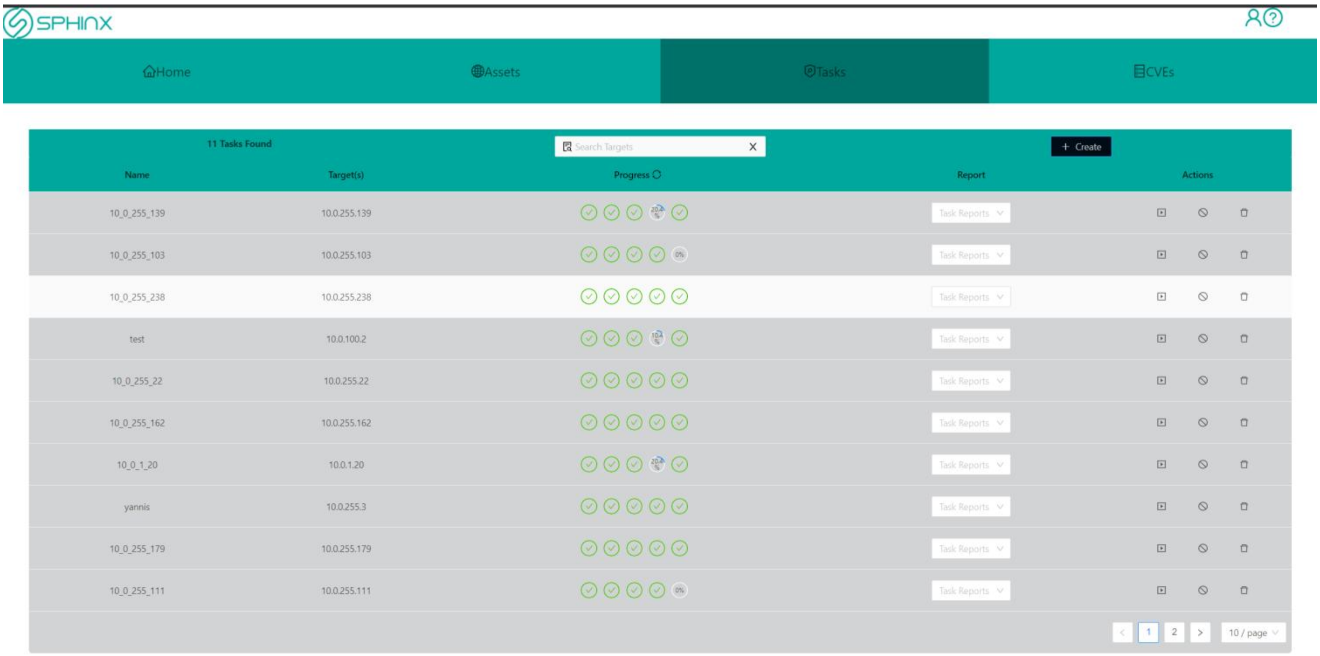
Figure 5 illustrates the Assets tab, wherein a user can check all of the assets found, various information regarding the assets (description, name, type, IP, MAC, etc.) and also from the **"Action"** column the user can edit the selected asset and delete it from the database. By clicking the **"Create"** button located on the top right of the component the user can create a new Asset.



Name	Description	Type	IP	MAC	Assessed	Modified	Value	Active	Vendor	Actions
			10.0.1.20	FA:E6:76:C7:7E:D0	true	14/04/21 12:36		true		
1			10.0.1.21	02:1F:D5:AA:A7:46	true	14/04/21 12:37		true		
			10.0.1.23	3A:02:12:64:19:F2	true	12/04/21 03:19		true		
			10.0.1.115	08:00:27:D1:57:AC	true	12/04/21 03:19		true	Oracle VirtualBox virtual NIC	
			10.0.1.150	6A:55:7C:FD:98:6C	true	12/04/21 03:22		true		
			10.0.1.155	08:00:27:44:B6:DB	true	12/04/21 03:22		true	Oracle VirtualBox virtual NIC	
			10.0.1.200	02:61:EE:B7:EC:A4	true	12/04/21 03:22		true		
			10.0.1.201	22:26:4A:31:6C:62	true	12/04/21 03:22		true		
			10.0.1.202	86:AE:1E:5F:94:0F	true	12/04/21 03:22		true		
			10.0.1.203	3A:D9:95:1E:3D:B2	true	12/04/21 03:22		true		

Figure 5 Assets Tab

The Tasks tab contains the vulnerability targets, their progress, the detailed vulnerability reports, and the actions for each task. Through the "**Actions**" column the user can restart a vulnerability assessment, stop the ongoing assessment, and delete it. The progress of each assessment is split into 5 subtasks, which are presented by 5 progress circles. The refresh button in the "**Progress**" column header refreshes the progress of the tasks. By clicking the **"Create"** button located on the top right of the component the user can create a new task assessment. Figure 6 depicts the Tasks tab.

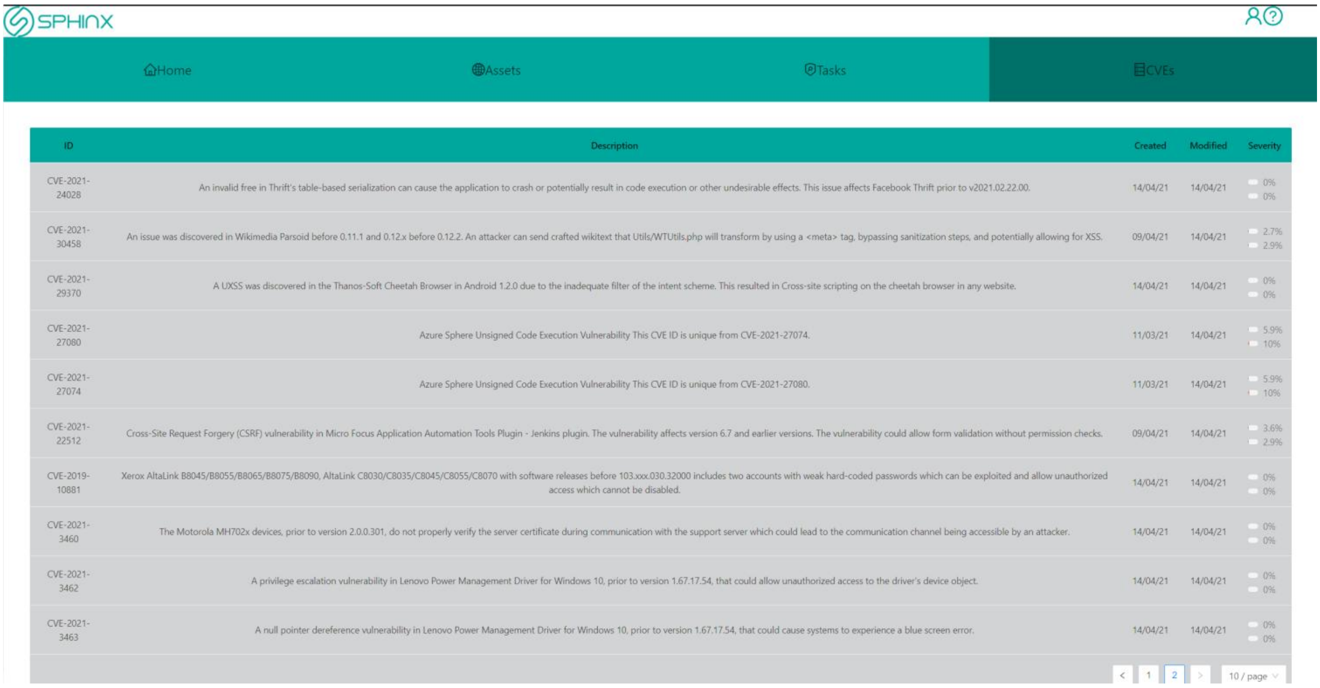


Name	Target(s)	Progress	Report	Actions
10_0_255_139	10.0.255.139	✓ ✓ ✓ 20% ✓	Task Reports	
10_0_255_103	10.0.255.103	✓ ✓ ✓ ✓ 0%	Task Reports	
10_0_255_238	10.0.255.238	✓ ✓ ✓ ✓ ✓	Task Reports	
test	10.0.100.2	✓ ✓ ✓ 10% ✓	Task Reports	
10_0_255_22	10.0.255.22	✓ ✓ ✓ ✓ ✓	Task Reports	
10_0_255_162	10.0.255.162	✓ ✓ ✓ ✓ ✓	Task Reports	
10_0_1_20	10.0.1.20	✓ ✓ ✓ 20% ✓	Task Reports	
yannis	10.0.255.3	✓ ✓ ✓ ✓ ✓	Task Reports	
10_0_255_179	10.0.255.179	✓ ✓ ✓ ✓ ✓	Task Reports	
10_0_255_111	10.0.255.111	✓ ✓ ✓ ✓ 0%	Task Reports	

Figure 6 Tasks Tab

The CVEs tab illustrates the latest available NVDs provided by NIST, wherein the user can see the ID of each CVE, its description, and the CVSS V3 and V2 severity of the CVE. Figure 7 depicts the CVEs tab.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.



ID	Description	Created	Modified	Severity
CVE-2021-24028	An invalid free in Thrift's table-based serialization can cause the application to crash or potentially result in code execution or other undesirable effects. This issue affects Facebook Thrift prior to v2021.02.22.00.	14/04/21	14/04/21	0% 0%
CVE-2021-30458	An issue was discovered in Wikimedia Parsoid before 0.11.1 and 0.12.x before 0.12.2. An attacker can send crafted wikitext that Utils/WTUtils.php will transform by using a <meta> tag, bypassing sanitization steps, and potentially allowing for XSS.	09/04/21	14/04/21	2.7% 2.9%
CVE-2021-29370	A UXSS was discovered in the Thanos-Soft Cheetah Browser in Android 1.2.0 due to the inadequate filter of the intent scheme. This resulted in Cross-site scripting on the cheetah browser in any website.	14/04/21	14/04/21	0% 0%
CVE-2021-27080	Azure Sphere Unsigned Code Execution Vulnerability This CVE ID is unique from CVE-2021-27074.	11/03/21	14/04/21	5.9% 10%
CVE-2021-27074	Azure Sphere Unsigned Code Execution Vulnerability This CVE ID is unique from CVE-2021-27080.	11/03/21	14/04/21	5.9% 10%
CVE-2021-22512	Cross-Site Request Forgery (CSRF) vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow form validation without permission checks.	09/04/21	14/04/21	3.6% 2.9%
CVE-2019-10881	Xerox AltaLink B8045/B8055/B8065/B8075/B8090, AltaLink C8030/C8035/C8045/C8055/C8070 with software releases before 103.xxx.030.32000 includes two accounts with weak hard-coded passwords which can be exploited and allow unauthorized access which cannot be disabled.	14/04/21	14/04/21	0% 0%
CVE-2021-3460	The Motorola MH702x devices, prior to version 2.0.0.301, do not properly verify the server certificate during communication with the support server which could lead to the communication channel being accessible by an attacker.	14/04/21	14/04/21	0% 0%
CVE-2021-3462	A privilege escalation vulnerability in Lenovo Power Management Driver for Windows 10, prior to version 1.67.17.54, that could allow unauthorized access to the driver's device object.	14/04/21	14/04/21	0% 0%
CVE-2021-3463	A null pointer dereference vulnerability in Lenovo Power Management Driver for Windows 10, prior to version 1.67.17.54, that could cause systems to experience a blue screen error.	14/04/21	14/04/21	0% 0%

Figure 7 CVEs tab

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.