A Multi-factor Assessment Mechanism to Define Priorities on Vulnerabilities affecting Healthcare Organizations

Gustavo Gonzalez-Granadillo[1], Rodrigo Diaz[1], Eleni Veroni[2] and Christos Xenakis[2]

[1]Atos Research & Innovation, Cybersecurity Unit, Spain,
[2]University of Pireus, Department of Digital Systems, Greece

Abstract

A key aspect on any risk assessment process is the identification and analysis of vulnerabilities associated to the target organization, its assets, services and devices. Considering that not all vulnerabilities are equally dangerous, and organizations cannot afford to blindly define strategies against the hundreds of newly discovered vulnerabilities, they must define priorities during the vulnerability management process. In addition, while many organizations base their prioritization of vulnerability management on scores such as the Common Vulnerability Scoring System (CVSS), a high portion of vulnerabilities associated to malware are scored with low or medium severity on the CVSS scale, which suggest that focusing only on CVEs which score high or critical would be a mistake. We propose in this paper a multi-factor assessment mechanism to define priorities of vulnerabilities affecting Healthcare Organizations. The mechanism helps classifying vulnerabilities based on their score and assigning priorities for their treatment.

Keywords

Vulnerability Discovery Manager, Vulnerability Assessment, Multi-factor Mechanism, Priority Assignment, Healthcare Organizations.

1. Introduction

With the discovery of new types of cyber-attacks and digital healthcare platforms being universally recognized as Critical Infrastructures, healthcare organizations realize the need to be technologically prepared against such challenges. Hospitals and healthcare centers have started taking actions to protect themselves inside the current landscape of attacks but most importantly to be able to react and mitigate new and unknown threats.

The health sector is exposed to a great number of threats that exploit vulnerabilities that in some cases are unknown by the target infrastructures. According to a recent report [1], vulnerabilities in healthcare IT infrastructure increased 341 percent between 2017 and 2018. In

ITASEC'21: Italian Conference on Cybersecurity, April 07–09, 2021, Online

gustavo.gonzalez@atos.net (G. Gonzalez-Granadillo); rodrigo.diaz@atos.net (R. Diaz); veroni@unipi.gr (E. Veroni); xenakis@unipi.gr (C. Xenakis)
https://ggranadillo.wixsite.com/english (G. Gonzalez-Granadillo); https://booklet.atosresearch.eu/rodrigo-diaz (R. Diaz); https://ssl.ds.unipi.gr/eleniveroni/ (E. Veroni); http://cgi.di.uoa.gr/~xenakis/ (C. Xenakis)
0000-0003-2036-981X (G. Gonzalez-Granadillo); 0000-0002-0946-4501 (E. Veroni); 0000-0001-6718-122X (C. Xenakis)

CEUR Workshop Proceedings (CEUR-WS.org)

addition, cyber attacks in the healthcare domain compromise not only network devices and data, but also applications and services supporting critical patient care systems. In this sense, healthcare centers must adopt new procedures to strengthen their systems and raise awareness among their employees .

One of the key phases in a vulnerability management process is the vulnerability analysis that aims to prioritize the risks to which organizations are exposed if a given vulnerability is successfully exploited. Considering that not all vulnerabilities are equally dangerous, and organizations cannot afford to blindly define strategies against the hundreds of newly discovered vulnerabilities, they must define priorities during the vulnerability management process. Prioritization is therefore, the key to a successful implementation of new vulnerability management programs [2, 3].

While many organizations base their prioritization of vulnerability management on scores such as the Common Vulnerability Scoring System (CVSS) [4], a high portion of vulnerabilities associated to malware are scored with low or medium severity on the CVSS scale, which suggest that focusing only on CVEs which score high or critical would be a mistake [5]. It is therefore important to develop new mechanisms of computing a vulnerability assessment based on multiple factors.

We propose a multi-factor assessment mechanism to define priorities of vulnerabilities affecting Healthcare Organizations. The mechanism is performed by a Vulnerability Discovery Manager (VDM) tool and will cover both cybersecurity and privacy vulnerabilities with a particular focus on health data, healthcare information systems and medical devices. The proposed approach is expected to help in the classification and prioritization of security vulnerabilities.

The remainder of this paper is organized as follows: Section 2 provides an overview of the vulnerability challenges identified in healthcare environments. Section 3 presents the Vulnerability Discovery Manager reference architecture by detailing its main components. Section 4 introduces the proposed multi-factor vulnerability assessment mechanism. Section 5 provides a use case example to show the applicability of the proposed mechanism. Section 6 provides related works. Finally, conclusions and perspectives for future work are provided in Section 7.

2. Vulnerability Challenges in the Healthcare Context

Much like any other domain where new technologies have emerged, healthcare faces increasingly more and more challenges to its cybersecurity. According to a recent study by Bugcrowd [6], between 2017 and 2018, the number of vulnerability submissions increased more than three times compared from previous years, from which around 30% had a critical severity. Healthcare organizations face most of their threats against their web site applications, with an average of 75% of the cases. This is mostly due to the fact that the medical practitioners as well as the manufacturers and developers providing said technologies do not often prioritize security. This, however, can be proven critical both to the health organization they work for and of course, to the patients' health and fundamental rights.

With no standards, guidelines and good practices communicated to all parties involved, and no known published examples of incidents in the industry until recently, as well as undisclosed details of such incidents where other vulnerabilities do not become known to the public or the industry, there is no standard way of making and using medical equipment handling data that will ensure security throughout its lifecycle. This leads to existing yet unknown vulnerabilities being either exposed, posing a threat to the reputation of the manufacturer and the provider, or worse, exploited, in which case personal and sensitive data can be compromised along with the smooth continuity of healthcare services provided. This can have critical consequences, such as major financial loss or even the loss of human life.

Additionally, until recently, a possibly false sense of safety was the norm in the healthcare industry, because it did not seem as a possible target for cyber-attacks. However, this changed ever since the medical records became electronic and are now stored and distributed online. The introduction of Electronic Medical Records (EMR) and Personal Medical Records (PMR), as well as the utilization of cloud services and storage, created a new attack surface for malicious parties. The value of such sensitive data, particularly on platforms where they would be exploited for identity theft or ransom, in combination with the lack of robustness of the security mechanisms of the healthcare infrastructures, pose an attractive target for attackers.

As no standard procedures have been established yet, the measures taken proactively by providers in order to protect their assets, may not be as effective. It has been observed that there are still healthcare organizations that have not created a cyber insurance policy taking into account security controls, nor have put their staff through cyber hygiene training, in fear that adding more security mechanisms to the system would interfere with their work. To overcome this, clear and strict procedures need to be established for all stakeholders who are part of the healthcare domain [7, 8, 9, 10, 11, 12].

Vulnerabilities in the Healthcare domain, originate due to a multiple number of causes [13]: (i) Most healthcare services and devices require single-factor authentication, making them a potential target to many threats (e.g., brute-force attacks); (ii) Some healthcare devices and apps share patient data with no data protection mechanisms, making them more vulnerable to attacks like Man-in-the-Middle (MITM); (iii) Errors and/or intentional incidents caused by insiders constitute one of the most common threat vectors in Healthcare organizations; (iv) Medical device security practices in place (e.g., code review, debugging systems and dynamic application security testing) lack of quality assurance and testing procedures [14]; (v) Disconnection between the perceptions of medical device manufacturers and healthcare practitioners about security implications of the medical equipment used; (vi) An important number of vendors and users do not disclose cybersecurity and privacy issues affecting their IoT medical devices, which block communications of vulnerabilities and threats in due time among healthcare organizations; (vii) Some medical devices run with outdated software and operating system.

3. Vulnerability Discovery Manager (VDM)

The Vulnerability Discovery Manager (VDM) is a domain-specific tool that identifies, analyses and manages vulnerabilities in the target infrastructure. VDM has been designed to support the key needs of the e-health sector (e.g., criticality and availability) aiming to: (i) identify vulnerabilities to system resources (discovery); (ii) classify and assign priorities to detected vulnerabilities (assessment); (iii) define remediation solutions to mitigate detected vulnerabilities (treatment); and (iv) provide intelligence sharing functionality in order to share the information with other hospitals and healthcare providers (sharing). In this paper we will focus on the assessment capabilities of the tool.

The VDM needs as input data the identification of the assets composing the target infrastructure. The discovery of the assets can be performed using any network scanner such as Nmap or a similar tool. The idea is to obtain information about the network and system devices (e.g., workstations, servers, printers, smartphones, etc.) to start the process of discovering vulnerabilities. Each device is identified by a unique IP address in the system, therefore having a list of IP addresses for all the elements (e.g., nodes, assets) composing the monitored system will trigger the analysis performed by the VDM.

As depicted in Figure 1 VDM has four main components: (i) vulnerability scanner, (ii) vulnerability storage, (iii) vulnerability assessment, and (iv) vulnerability reporting and sharing. The remainder of this section details each VDM component.

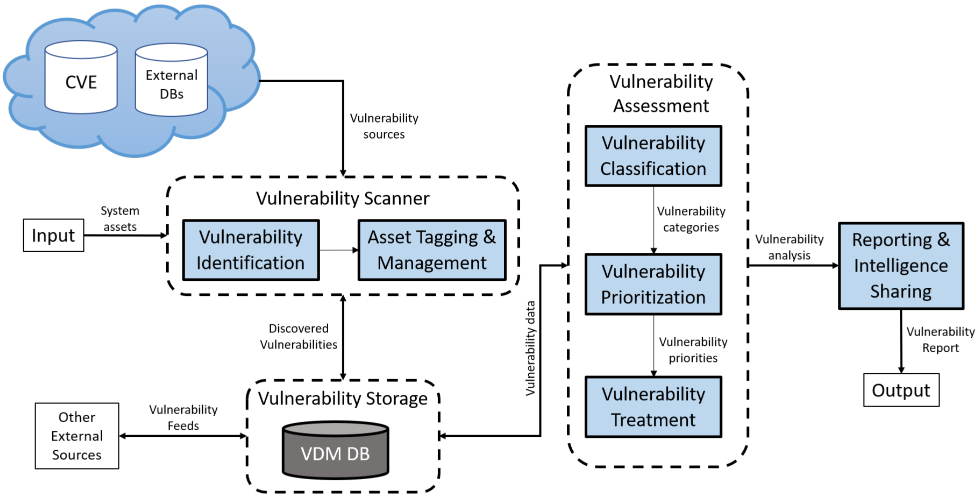

Figure 1: Vulnerability Discovery Manager Architecture

3.1. Vulnerability Scanner

This module is in charge of discovering and associating vulnerabilities to the list of nodes present in the input file. It is composed of two main processes: (i) vulnerability identification; and (ii) asset tagging and management. After the identification of vulnerabilities, the tool will associate each node/asset with its corresponding vulnerabilities. This process allows to verify that vulnerabilities match the assets (e.g., devices, equipment, software) in the target network. The objective of this process is to reduce the number of false positives or negatives and to concentrate on the system's exploitable weaknesses. The outcome of this process is a list of assets and associated vulnerabilities that will be stored in the VDM database and assessed in the next modules.

3.2. Vulnerability Storage

The VDM DB is a central component that stores the JSON files generated by the vulnerability scanner module. Examples of this information include CVEs, CWEs, CVSS, vulnerability descriptions, attack patterns, related assets, and relevant information associated to the detected vulnerabilities from all assets composing the target system. The VDM DB is the connection entity among all VDM components (i.e., Vulnerability scanner, assessment, reporting & sharing). The VDM DB allows the retrieval of vulnerabilities and risk information related to assets composing the target infrastructure.

3.3. Vulnerability Assessment

This module analyzes the list of detected vulnerabilities, classifies them according to their category, assigns them priorities based on their risk levels and provides treatment to avoid/mitigate them. Details on the Vulnerability Assessment process is provided in Section 4. Based on the obtained score, the risk associated to a given vulnerability can be classified as: (i) Critical, $VA >= 4.1$; (ii) High, $3.1 >= VA <= 4.0$; (iii) Medium, $2.1 >= VA <= 3.0$; (iv) Low, $1.1 >= VA <= 2.0$ and (v) Negligible, $0.0 >= VA <= 1.0$.

3.4. Reporting and Intelligence Sharing

The VDM tool produces a vulnerability report with valuable information about the target network/hosts and their associated vulnerabilities. The report is stored in the VDM DB and can be displayed in a dashboard or exported in PDF, or STIX[1] format. This latter uses STIX objects (e.g., event objects) that can also be integrated in the VDM DB. An Event object describes a dynamic observable cyber event (e.g., the occurrence of an attack). Healthcare organizations have the possibility to share their vulnerability results and new discoveries with other organizations, communities and research groups using the Malware Information Sharing Platform (MISP[2]) as the reporting and intelligence sharing platform.

4. Multi-factor Assessment Mechanism

The Vulnerability Assessment (VA) value is a metric that comprises three main parameters: (i) Root cause, (ii) Impact, and (iii) Remediation, as shown in Equation 1.

$$VA = \frac{Root\_cause + Impact + Remediation}{n} \tag{1}$$

Please note that "n" corresponds to the number of parameters composing the equation from which the value is different from null. If information is not available in any of the parameter, it will be discarded from the analysis. The remainder of this section details the identification of each of the parameters composing Equation 1 .

[1] https://stixproject.github.io/

[2] https://www.misp-project.org/

4.1. Root Cause

It identifies the main root causes of security vulnerabilities. The cause can be known or unknown. Known causes can be further classified as complexity, open connections, weak passwords, design flaws, and human factor (as shown in Table 1) [15, 16].

Root Cause	Description	Score
Human Factor	Vulnerabilities caused due to insufficient training, unawareness, and lack of experience, causing coding errors and improper management of assets and data.	5
Design Flaws	Design flaws and bugs in software and hardware. Example: Bugs in widely used operating systems and browsers can expose millions of businesses to significant risks.	4
Failures	Ordinary malfunctions and hardware/software failures due to technical issues that could lead to a denial of service of the system.	4
Complexity	Security vulnerabilities rise proportionally with complexity. Complex software, hardware, information, businesses and processes can all introduce security vulnerabilities.	3
Weak Passwords	Passwords are used to secure virtually everything: mobile devices, software, websites, company VPNs and enterprise software. Despite education about the dangers — many people still write passwords down, share them or give them out to websites.	3
Open Connections	Each open connection is a potential avenue for exploitation. Examples: wired internet, mobile devices, WiFi, open ports, etc.	2
Unknown	No information is available to assess this parameter.	-

Table 1
Root Cause Detailed Information

4.2. Vulnerability Impact

It assesses the potential impact of a given vulnerability if successfully exploited on the target system/network. It considers three main aspects: (i) data at risk, (ii) severity, and (iii) damage.

4.2.1. Data at risk:

It identifies and assesses the type of information that needs protection in the organization e.g., Personally Identifiable Information (PII), Intellectual Property Data (IPD), Financial Data, Social Media, etc. (as shown in Table 2) [17, 18].

4.2.2. Severity:

It considers the CVSS base metric group that represents intrinsic characteristics and severity of a vulnerability that are constant over time and across user environments. It is composed of exploitability metrics (e.g., attack vector, attack complexity, privileges required, user interaction); and impact metrics (i.e., confidentiality, integrity, availability).

Based on the CVSS results, vulnerabilities are assigned a severity score as follows: None: no severity with CVSS = 0.0 (severity = 1), Low: $0.1 >= CVSS <= 3.9$ (Severity =2), Medium:

Data at Risk	Description	Score
PII	Data that could potentially identify a specific individual, e.g., medical information, birth date, social security numbers, citizen ID, etc.	5
Financial Data	Related to the offering or delivery of a financial product/service or processing of a purchase (e.g., credit card, bank account, loan, etc.).	5
IPD	It refers to sales and marketing plans, new product plans, patents, customer and supplier information, etc.	5
Social media accounts	It refers to information often used for authenticating to various applications and proving a user's identity.	4
Third-party data	It refers to any kind of data accessed, handled and/or supplied by third parties.	3
Social network data	It refers to data about the vulnerable organization/product that is publicly available in social networks, blogs and public websites.	2
Unknown	No information is available to assess this parameter.	-

Table 2
Data at Risk Detailed Information

4.0 $>=$ $CVSS$ $<=$ 6.9 (Severity=3), High: 7.0 $>=$ $CVSS$ $<=$ 8.9 (Severity = 4), and Critical: $CVSS$ $>=$ 9.0 (Severity = 5).

4.2.3. Damage:

It considers the potential damage that could be caused by a breach of the affected system if the vulnerability is successfully exploited (as seen in Table 3).

Damage	Description	Score
Total Damage	The system is expected to be highly damaged due to the successful exploitation of the vulnerability.	5
Partial Damage	The system is expected to be partially damaged due to the successful exploitation of the vulnerability.	3
NO/Low Damage	The system is not expected to be damaged due to the successful exploitation of the vulnerability.	1
Unknown	No information is available to assess this parameter.	-

Table 3
Damage Detailed Information

The vulnerability impact is a metric composed of three parameters: (i) the data at risk, (ii) the severity, and (iii) the damage (as shown in Equation 2).

$$Impact = \frac{Data\_at\_Risk + Severity + Damage}{n} \tag{2}$$

Please note that "n" corresponds to the number of parameters composing the equation from which the values are different from null. If information is not available in any of the parameter composing this metric, such parameter will not be considered in the analysis.

4.3. Remediation

It assesses the potential capabilities for an organization to implement and recover for a successful exploitation of a given vulnerability in its system. It considers the recovery time, requirements, resilience, costs and recovery level.

4.3.1. Recovery Time:

It identifies and assesses the time needed for an infrastructure to recover from a given attack, assuming the vulnerability is successfully exploited by a malicious entity (as seen in Table 4).

Recovery Time	Description	Score
Long	The system requires a long period of time to be completely recovered from an attack (usually within weeks or months).	5
Medium	The system can be recovered from an attack in a period of time longer than 24hrs (usually within days).	3
Short	The system can be easily recovered from an attack in a short period of time (usually within hours).	1
Unknown	No information is available to assess this parameter.	-

Table 4
Recovery Time Detailed Information

4.3.2. Requirements:

It identifies and assesses the type of security measures (e.g., protective, reactive) the target system needs to implement in order to recover from a given attack (as seen in Table 5).

Requirements	Description	Score
New measures	The system requires implementing new reactive or protective measures).	5
Existing measures	The system requires implementing existing measures.	3
No measure	The system does not require to implement any measure.	1
Unknown	No information is available to assess this parameter.	-

Table 5
Requirements Detailed Information

4.3.3. Resilience:

It identifies and assesses the actions needed by the target system to keep running after a vulnerability has been detected and/or exploited (as seen in Table 6).

4.3.4. Cost:

It identifies and assesses the actions needed by the target system to keep running after a vulnerability has been detected and/or exploited (as seen in Table 7).

Resilience	Description	Score
Low	The system requires to remove the vulnerability to keep running.	5
Medium	The system does not require to remove the vulnerability, but its removal is highly recommended to keep running.	3
High	No need to remove the vulnerability to keep running.	1
Unknown	No information is available to assess this parameter.	-

Table 6
Resilience Detailed Information

Cost	Description	Score
High	Measures are implemented at a high cost and require great effort.	5
Medium	Measures are implemented at a moderate cost and require some effort.	3
Low	Measures can be implemented at no cost (or low cost) and does not require too much effort.	1
Unknown	No information is available to assess this parameter.	-

Table 7
Cost Detailed Information

4.3.5. Recovery Level:

It identifies and assesses level of recovery expected for the target system after the implementation of security measures (as seen in Table 8).

Recovery	Description	Score
No recovery	After implementing a mitigation measure, the system is expected to be not operative.	5
Partial recovery	After implementing a mitigation measure, the system is expected to be partially operative.	3
Total recovery	After the implementation of a mitigation measure, the system is expected to be fully operative.	1
Unknown	No information is available to assess this parameter.	-

Table 8
Recovery Detailed Information

The remediation score is therefore computed as the average of the recovery time, requirements, resilience, cost and recovery level parameters, as shown in Equation 3.

$$Remediation = \frac{Recovery\_Time + Requirements + Resilience + Cost + Recovery\_Level}{n} \quad (3)$$

Please note that “n” corresponds to the number of parameters composing the equation from which the value is different from null. If information is not available in any of the parameter composing this metric, such parameter will not be considered in the analysis.

5. Example of Usage

Considering a vulnerability of a remote code execution detected in a server from a healthcare organization (as shown in Annex A), the first step on the vulnerability assessment process is to identify the root cause. Although this is not clearly specified in the provided information, a remote code execution can be associated to multiple causes (e.g., open connections, weak passwords, complexity, design flaws, human factors, or a combination of some of them), therefore, the *Root_cause* score is set to five (5).

The second step is to compute the vulnerability impact. Considering that the vulnerability is associated to a hospital server, the remote code execution could lead to the identification of personal data (e.g., medical information), therefore the *Data_at_risk* score is set to five (5). In addition, the CVSS value for this vulnerability is equivalent to ten (10), therefore, the $Severity$ score is set to five (5), and since the system is expected to be partially damaged due to the successful exploitation of the vulnerability, its *Damage* score is set to three (3). As a result, the $Impact$ value for this vulnerability is 4.33.

The third step is to compute the vulnerability remediation value. For that, the following assumptions have been made:

- The system can be easily recovered in a short period of time ($Recovery\_Time$ = 1)
- The system requires implementing new security measures ($Requirements$ = 5)
- The system does not need to remove the vulnerability to keep running (*Resilience* = 1)
- No information is available to assess the cost parameter (*Cost* = 0). This parameter is therefore not considered in the score calculation.
- After the implementation of a mitigation measure, the system is expected to be fully operative ($Recovery\_Level$ =1)

Therefore, the *Remediation* score is equivalent to 2.

The final step consists on calculating the Vulnerability Assessment (VA) and classification. As a result, $VA = 3.78$, which corresponds to a HIGH priority.

6. Related Work

Novel approaches and tools based on old and recent technologies aim to filling possible security gaps underlying in modern healthcare cyber solutions. However, while it is important to safeguard the digital infrastructures from those who threaten them, it is also important to do so without disrupting the continuous healthcare procedures, or making them too complex to use for people with no technical background, such as the patients and the medical staff. To protect healthcare organizations, a cybersecurity solution needs to be in position to monitor and control all the security-critical aspects. Several solutions to identify and detect vulnerabilities in healthcare infrastructures have been proposed so far, nonetheless, few of them perform a thorough approach to assess and classify their severity.

The Cybersecurity and Infrastructure Security Agency (CISA[3]) has initiated an effort to enhance security, resiliency and reliability of the Nation's cybersecurity and communication

[3] https://www.cisa.gov/

infrastructure. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[4]) is a CISA initiative that provides a control system security focus in collaboration with US-CERT to conduct vulnerability and malware analysis, share and coordinate vulnerability information and threat analysis through information products and alerts, among other services.

Commercial solutions (e.g., Bugcrowd's crowdsourced security [19]) are available in the market to help healthcare organizations to discover and manage critical vulnerabilities in the health sector. The solution enables healthcare professionals to assess the risk associated with disparate data sources and infrastructure and ensures compliance with the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Other well-known commercial and open-source solutions (e.g., Nessus[5], OpenVAS[6]) provide vulnerability assessment capabilities that strongly depend on the CVSS results.

A vulnerability database containing timely information about current security issues, weaknesses, vulnerabilities and exploits on industrial control systems is publicly available as part of the CISA services and frequently updated by ICS-CERT advisories. Similar to the CVE database, the ICS-CERT Advisories database provides a list of industrial control system vulnerabilities. However, several issues have been recently identified [20]: (i) The provided recommendations are generic and, in some cases, meaningless; (ii) Industrial impact is ignored; (iii) Likelihood of exposure is missing; (iv) Some advisories contain errors in the CVE and CVSS score; (v) It may take months or years to get to a resolution; and (vi) Some vulnerabilities may not be mitigable besides patching, and some of them provide no advice at all.

In order to cope with the aforementioned shortcomings, we propose a vulnerability discovery manager that uses a multi-factor assessment mechanism to define priorities on vulnerabilities affecting critical infrastructures with a particular focus on healthcare organizations.

7. Conclusions

This paper presents a multi-factor assessment mechanism to classify define priorities of vulnerabilities affecting Healthcare infrastructures. It details a tool named Vulnerability Discovery Manager (VDM) which is composed of four main modules: (i) a vulnerability scanner, to check for vulnerabilities of the target nodes; (ii) a vulnerability storage, to save discovered vulnerabilities in a local database; (iii) a vulnerability assessment, to prioritize vulnerabilities and provide mitigation guidance; and (iv) a report and intelligence sharing, to communicate and share VDM output with other healthcare institutions.

The proposed assessment mechanism considers not only the vulnerability root causes, but also its impact and potential remediation actions to be implemented. As a result, a score ranging form zero to five is assigned to a particular vulnerability and shared in a platform where other healthcare centers and research organizations can benefit.

An example of usage is provided in Section 5 to show the applicability of our proposed mechanism over a vulnerability report generated by the VDM in a JSON format. Future work will focus on evaluating other factors and refining current values used to compute the vulnerability

[4] https://us-cert.cisa.gov/ics

[5] https://www.tenable.com/products/nessus

[6] https://www.openvas.org/

assessment score.

8. Acknowledgments

The research work presented in this article has been supported by the European Commission under the H2020 Programme, through funding of the "CUREX: seCUre and pRivate hEalth data eXchange" project (G.A. id: 826404).

Acknowledgments

Thanks to the developers of ACM consolidated LaTeX styles https://github.com/borisveytsman/acmart and to the developers of Elsevier updated LaTeX templates https://www.ctan.org/tex-archive/macros/latex/contrib/els-cas-templates.

References

[1] F. Donovan, Reports of healthcare it infrastructure vulnerabilities surge 341%, [online], 2019. https://hitinfrastructure.com/news/reports-of-healthcare-it-infrastructure-vulnerabilities-surge-341.

[2] Ayala Goldstein, The future of vulnerability management programs, [online], 2018. https://resources.whitesourcesoftware.com/blog-whitesource/the-future-of-vulnerability-management-programs.

[3] Ayala Goldstein, Vulnerability management - what you need to know, [online], 2020. https://resources.whitesourcesoftware.com/blog-whitesource/vulnerability-management.

[4] FIRST, Common vulnerability scoring system v3.1: Specification document, [online], last visited February 2021. https://www.first.org/cvss/v3.1/specification-document.

[5] NOPSEC, State of vulnerability risk management report, [online], 2018. http://info.nopsec.com/rs/736-UGK-525/images/NopSec_2018_SOV_Report.pdf.

[6] Bugcrowd, State of healthcare security in 2019, [online], 2019. https://www.bugcrowd.com/blog/state-of-healthcare-security/.

[7] N. Y., P. E., M. G., M. C. X., S. C., M. E. K., Vulnerability assessment as a service for fog-centric ict ecosystems: A healthcare use case 12 (2019) 1216–1224.

[8] S. S., M. A. M., M. E. K. J., S. Z. (Eds.), Cyber Vulnerabilities on Smart Healthcare, Review and Solutions, IEEE Cyber Resilience Conference (CRC), 2018.

[9] S. A., K. V., U. D. (Eds.), Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities, IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2018.

[10] D. D. I., D. I. (Eds.), Cyber security in healthcare networks, IEEE E-Health and Bioengineering Conference (EHB), 2017.

[11] K. D., F. K., G. C., R. A., Security for mobile and cloud frontiers in healthcare 58 (2015) 21–23.

[12] S. M., N. Y., P. S., P. E., E. K. Markakis (Eds.), A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues, IEEE Communications Surveys & Tutorials, 2020.

[13] Health Tech Staff, Ho healthcare can pinpoint common vulnerabilities – and build defenses, [online], 2018. https://healthtechmagazine.net/article/2018/07/how-healthcare-can-pinpoint-common-vulnerabilities-and-build-defenses.

[14] Ponemon Institute, Medical device security: An industry under attack and unprepared to defend, [online], 2017. https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf.

[15] John Spacey, The 10 root causes of security vulnerabilities, [online], 2013. https://arch.simplicable.com/arch/new/10-root-causes-of-security-vulnerabilites.

[16] A. V. Revnivykh, A. Fedotov, Root causes of information systems vulnerabilities 8 (2015).

[17] European for Information Technology, 3 types of data that need protection, [online], last visited February 2021. https://europeanitc.com/the-quick-brown-fox/.

[18] Joseph Streinberg, 12 types of data that businesses need to protect but often do not, [online], 2018. https://josephsteinberg.com/12-types-of-data-that-businesses-need-to-protect-but-often-do-not/.

[19] Bugcrowd, Why healthcare it should include crowdsourced security, [online], 2019. https://www.bugcrowd.com/blog/why-healthcare-it-should-include-crowdsourced-security/.

[20] Dragos, Industrial controls system vulnerabilities, [online], 2018. https://dragos.com/wp-content/uploads/yir-ics-vulnerabilities-2018.pdf.

A. Extract from a VDM report in JSON format

```
{
 ”vulnerability”: {
 ”type”: ”vulnerability”,
 ”id”: ”64abb211-63ff-4397-8966-32ca1dbf691b”,
 ”created”: ”2021-01-19T16:24:59.410559Z”,
 ”modified”: ”2021-01-19T16:24:59.410559Z”,
 ”name”: ”Remote Code Execution”,
 ”description”: ”The Treck TCP/IP stack before 6.0.1.66 allows Remote
  Code Execution, related to IPv4 tunneling.”,
 ”labels”: [
 ”General”
 ]
 ”external_references”: [{
     ”source_name”: ”cve”,
     ”url”: ”https://tools.cisco.com/security/center/content/Cisco
       SecurityAdvisory/cisco-sa-treck-ip-stack-JyBQ5GyC,
       https://www.kb.cert.org/vuls/id/257161/,https://www.treck.com”,
     ”hashes”: {
```

```
    "SHA-256": "453e1635c745693a99d74645101b45de40de919b04b9c49f
     d91e30b1ee001fc4"
        },
    "external_id": "CVE-2020-11896"
    }       ],     },
  "report_scan": {
    "type": "report",
    "id": "4a446cc6-2d2c-4f72-a176-1609af7b9488",
    "start_scan": "2021-01-19T16:24:54.336+00:00",
    "end_scan": "2021-01-19T16:24:59.353+00:00",
    "profile": "Full and fast",
    "host": "10.0.2.6",
    "name": "Remote Code Execution",
    "description": "The Treck TCP/IP stack before 6.0.1.66 allows
     Remote Code Execution, related to IPv4 tunneling.",
    "threat": "High",
    "severity": "10.0",
    "port": {
      "number": 0,
      "proto": "tcp",
      "name": "general"
    },
    "nvt": {
      "name": "Remote Code Execution",
      "family": "General",
      "cvss_base": 10.0,
      "cve": ["CVE-2020-11896"],
      "impact": "",
      "summary": "The Treck TCP/IP stack before 6.0.1.66 allows
       Remote Code Execution, related to IPv4 tunneling.",
      "solution": "",
      "solution_type": "VendorFix",
      "affected": "",
      "vuldetect": "",
      "insight": "",
      "cvss_details": {
        "AV": "N",
        "AC": "L",
        "Au": "N",
        "C": "C",
        "I": "C",
        "A": "C"
      }         }        }     }
```