International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
https://ijemr.vandanapublications.com

Peer Reviewed & Refereed Journal
Volume-13, Issue-5 (October 2023)
https://doi.org/10.31033/ijemr.13.5.11

Patching Vulnerabilities to Improve the Security Posture in the Financial Transactions

Kamal Aldin Yousif Yaseen
Department of Information System, CEMIS College, University of Nizwa, Nizwa, OMAN

Corresponding Author: k.yousif@unizwa.edu.om

Received: 01-10-2023 Revised: 15-10-2023 Accepted: 29-10-2023

ABSTRACT

An organization's security posture is the security status of all its networks, data, people, and systems; the resources it employs to protect them; and its ability to defend against attacks and quickly recover from them, patching vulnerabilities can minimize the investment cost but only a small reduction in the system risk. Therefore, efficient security assessment methods are needed that are not model or metric oriented, as well as an equivalent accuracy with respect to evaluating all possible attack scenarios.

This paper contribution will be more focused on the security posture by explaining its importance, tools, for vulnerability patching, and their huge impact on enhancing the security situation in financial organizations.

Keywords**—**Vulnerability, Patching, Risk, Transaction, Cybersecurity, Protection

1. INTRODUCTION

Cyber-attacks have had a severe impact on our daily lives, especially for financial institutions, as they target the infrastructure of various business networks, all the way to private networks in homes and institutions. Cyberattacks have become more complex and impactful in terms of attack patterns, types and methods, which makes it difficult for our task to design methods of defending networks and other services related to them. Those in charge of cybersecurity in organizations must understand its requirements more, especially with regard to collective vulnerabilities and not just individual vulnerabilities with limited impact. Accordingly, the three security requirements of confidentiality, privacy, and availability (also known as the CIA triad) must be fulfilled. Rigorous security assessments can also identify attack scenarios and associated vulnerabilities, which can be effectively secured using mitigation scenarios. For example, an Advanced Persistent Threat (APT) attack also violates a networked system. Hence Distributed Denial of Service (DDoS) attack It is necessary to conduct in-depth security assessments of networked systems to identify critical attack scenarios and deploy effective mitigation strategies to reduce the impact of cyber-attacks while ensuring the CIA of the networked system [1]. Vulnerability patching is a vital mitigation strategy any organization should enable to avoid and reduce cybersecurity issues, Software vulnerabilities are a major threat to organizations today. The cost of these threats is significant, both financially and in terms of reputation, Vulnerability management and patching can easily get out of hand when the number of vulnerabilities in your organization is in the hundreds of thousands of vulnerabilities and tracked in inefficient ways, such as using Excel spreadsheets or multiple reports, especially when many teams are involved in the organization [2].

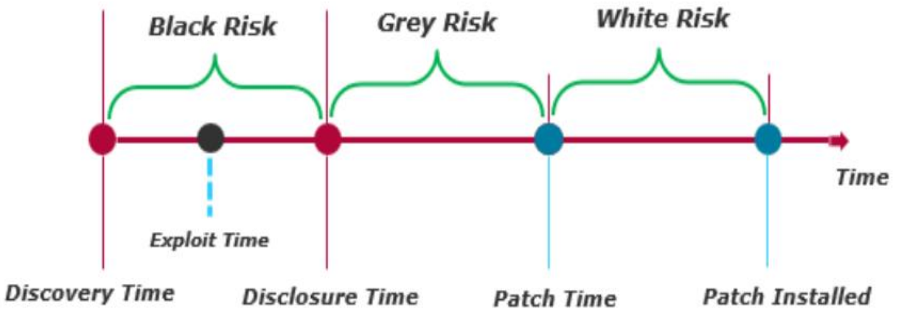

Figure 1: Vulnerability Lifecycle

Even after the process of correcting and patching vulnerabilities, organizations are still struggling to effectively correct and repair vulnerabilities in their assets. This is because teams place the severity of security vulnerabilities as a top priority and prefer to apply patches to vulnerabilities

This work is licensed under Creative Commons Attribution 4.0 International License.

according to the following classifications: Critical > High > Medium > Low > Information. The following sections explain why this approach is flawed and suggest how we can improve it so that the number of reports that must be sifted to prioritize corrections can be increased significantly in a relatively short period of time, and if a group of teams are involved, this increases the complexity and time required to complete and coordinate corrections. And determine their priorities. To make matters worse, new exploits continue to appear almost daily and keeping track of new exploits and available patches can become a huge task that can quickly get out of control if not handled properly. Unless an organization has a very mature security program, it will be difficult to manage patching effectively, and simplifying patching requires you to simplify prioritization first. A "risk-based approach" means that you will evaluate the potential impact of the vulnerability against the likelihood of it being exploited. This allows you to decide whether it is worth taking action or not. To simplify prioritization, consider the following the exposure of the asset [3][4].

- The business sensitivity of the asset.
- The severity of the vulnerability reported against the asset.
- The availability of an exploit for the vulnerability reported.
- The complexity of the exploit, if it is available.
- The taxonomy of the vulnerability reported.

A robust cybersecurity permissions have now become a requirement for all organizations, especially financial ones, such as firewalls, anti-hacker and anti-malware programs (IDS, NIDS), email filters, web pages, endpoint and network detection and response systems, in addition to cloud security solutions. Security teams also make extensive use of intelligence-backed tools. Artificial intelligence to continue monitoring networks around the clock and neutralize dangerous attacks expected to occur. Automating threat detection and mitigation creates a more proactive cybersecurity posture and provides some relief to overworked and understaffed security teams. Below I'll suggest some technical solutions to correct:

1.1 Monitor Critical Security Vulnerabilities

Cybercriminals are constantly adapting their means and methods of attack. To protect against evolving threats, your security team needs to continuously monitor and gauge whether your IT systems are vulnerable to new forms of attack. intelligence feeds that distribute information on active exploits and cyber gangs can help organizations proactively protect their networks and identify the latest threats.

1.2 Adopt a Zero-Trust Framework

A May 2021 presidential executive order called for federal agencies to implement a zero-trust framework, which required all users of federal computer networks to be continuously authenticated when using network resources, and to only have access to the apps, data, and systems they need to do their jobs. This makes it much harder for attackers who have breached the perimeter to move laterally through the network. According to a September 2022 survey by Okta, more than half of enterprises have zero-trust initiatives currently underway, while many more plan to launch initiatives within the next 12 to 18 months.

1.3 Transition to a DevSecOps Approach

Adopting a DevSecOps approach integrates security into the process of software development and deployment. Security personnel can quickly identify and mitigate potential vulnerabilities before code is shipped, avoiding expensive and time-consuming rework, as well as preventing insecure code from inadvertently being deployed in production. A key element of this approach is red teaming—looking at code from the point of view of an attacker to isolate its strengths and weaknesses.

1.4 Implement Cybersecurity Training for all Employees

More than 8 out of 10 security breaches are the result of human error—from employees revealing their log-in credentials by phishing emails, a manager losing a laptop or phone containing sensitive corporate data, or an admin misconfiguring server settings to allow public access to proprietary intellectual property. Top executives in particular are prime targets for "spear phishing," in which emails impersonate them, and other direct attacks seeking their access credentials. Educating all employees in cybersecurity fundamentals can minimize an organization's exposure to social engineering attacks and malware infestations, reducing its overall vulnerability. Simulated phishing attacks can identify which employees are most susceptible and in need of further training. Teaching employees how to recognize and report attacks can reduce response times—a key element in successful mitigation[5].

1.5 Develop and Practice an Incident Management Plan

It's inevitable that your organization will eventually fall victim to an attack or suffer a data breach. Proactive security posture management requires having an incident management plan in place to identify, analyse, and resolve such critical incidents. The plan needs to outline the appropriate responses for each department head and detail their procedures and roles. Just as important, the plan can't simply sit on a shelf—it needs to be practiced, via table-top exercises or simulated attacks, and be regularly updated as threats evolve [6].

1.6 Protection of Financial Transactions and Online Purchases

To protect confidential data such as (passwords and bank card numbers) that we enter into banks and payment systems and to prevent money theft and fraud when making payments via the Internet, sites ask you to open them using reliable protection programs such as Kaspersky Internet Security or any of the effective protected browsing programs.

This work is licensed under Creative Commons Attribution 4.0 International License.

Protected browsing mode is considered one of the special operating modes that provides the greatest amount of effective protection during browsing, specially completing transactions and payment procedures. It is also run in a separate environment from other applications for greater protection so that these applications are not able to pass any instructions during the payment process, as browsers such as (Google Chrome and Mozilla Firefox) creates special profile files for the same purpose, in addition to automatically switching the browser to protected mode when you visit banking sites and sites that involve conducting financial transactions and opening a completely new window to be able to conduct transactions in a secure manner[7]. The following is the capability of the protected browser:

Untrusted modules. The application runs a check for untrusted modules every time you visit a bank or payment system website.

- **Rootkits.** The application scans for rootkits at Protected Browser start-up.
- **Known Operating System Vulnerabilities.** The application scans for operating system vulnerabilities at Protected Browser start-up.
- **Invalid Certificates of Bank or Payment System Websites.** The application checks certificates when you visit a bank or payment system website. The check is performed against a database of compromised certificates.

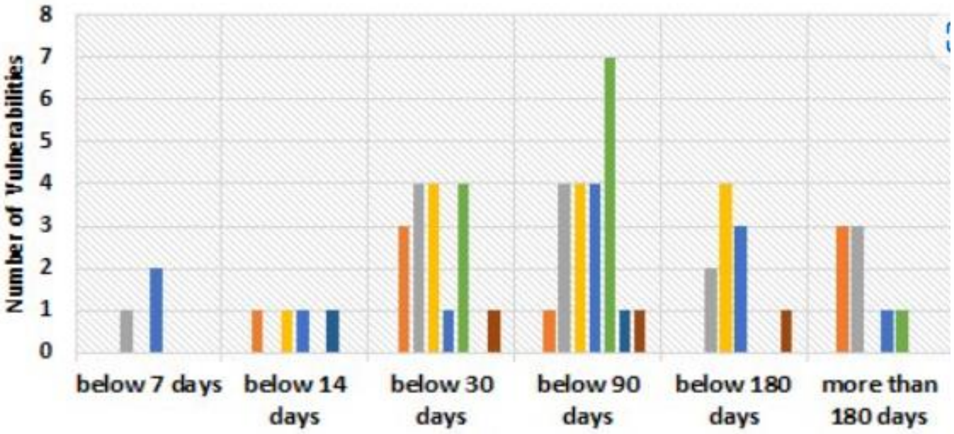

Figure 2: Vulnerabilities that are patched after Disclosure Time for OpenStack releases

II. RELATED WORKS

The frequency of information security incidents has increased significantly and alarmingly in recent years, which has negatively affected the efficiency of the operations of companies and financial institutions and has led to very large losses and damages. In most cases, faulty configurations in systems and networks and unprotected weak points [8] are attacked as a result of attackers using different and sophisticated tactics. Which had a negative impact on information security and economies [9] According to the Arab International Journal of Information Security, the rate of attacks was more than 286 incidents or damages to information security in one day, which led to paralysis in networks, taking advantage of the weakness of servers and vulnerabilities in operating systems and applications. Being the reasons to system getting: Accessed, modified and shut-down out of the security policy in organizations [10]. Arbaugh et al. [11] presented a vulnerability life-cycle model. In general, the vulnerability timeline is starting from the discovery of software vulnerability until the patch is deployed. When software vendors release the patch in response to the weakness of the system, the user can then apply it to solve the issue. [3, 7, 13,]. Consequently, Brykczynski and Small [8] reported practices of security patch management and also, emphasized an importance of economic security patch management as a part of information asset management.

III. GOALS

1. Understand the importance of patching.
2. Establish a patching schedule.
3. Establish and execute on a policy for systems that need additional approvals prior to patching.

1. Establish a formal patch management plan leveraging automated tools and aligned with your asset management plan.

IV. METHODOLOGY& FRAMEWORK

Here 1 introduce my proposed framework to mitigate the risks characterized in Section V-D. i aggregate and correlate information from NVD, OLB and OSVDB, EDB and SymDB. EDB[11] is an open repository for proof-of-concept exploits while SymDB, is an open database of vulnerabilities exploited in the wild. EDB and SymDB have been used for quantitative security assessments, but i apply these to create a

This work is licensed under Creative Commons Attribution 4.0 International License.

knowledge base for generating vulnerability signatures/plugins. The first three databases were already introduced in Section IV-A. We leverage on OpenVAS [14] scanning engine for the actual vulnerability scanning. OpenVAS is a popular open source vulnerability scanning framework consisting of several tools used for security assessment. At the lower level, identification of software flaws is done by the NVTs or plugins. Open Vulnerability Assessment System (OpenVAS) currently employs about 40,627 plugins. These plugins are developed using Nessus Attack Scripting Language (NASL), a scripting language originally developed for Nessus vulnerability scanner[14].

V. DISCUSSION

In Figure 2, the graph shows the number of security vulnerabilities that were patched after the time versions were disclosed, what distinguishes the vulnerability update policy of OpenStack is that it is multi-functional and requires transferring the device vulnerabilities to the adequate engineer for the actual available resources. Therefore, the subject of this study is choosing the appropriate system, as the main goal of this protocol is that by transferring the simple threat to the second-level specialists to update the patch, it makes it possible to Addressing the previous problems with very important resources, and thus the vulnerability of the device. In this study, I propose to reduce the dwell time to a minimum and improve the efficiency of updating the patch. To accomplish this, I build the problem in a mathematical model, which is a patch assignment algorithm, which is ideal for security vulnerabilities to research in the process of reducing time and increasing Efficiency in the case of non-linear and non-convex integer programming. Vulnerabilities remain in the device before updating the patch. Thus, backup devices must be considered for IT support centers, their load settings must be changed, and the working hours of their employees must be considered at their maximum. Moreover, in order to build the mathematical model, the complexity of the equation must be avoided. I made an assumption in advance that “each vulnerability is addressed by a single IT support center” and handled by “a single information security specialist.” Thus, the problem is simplified, easier to contain, and the cost consideration of other assumptions.

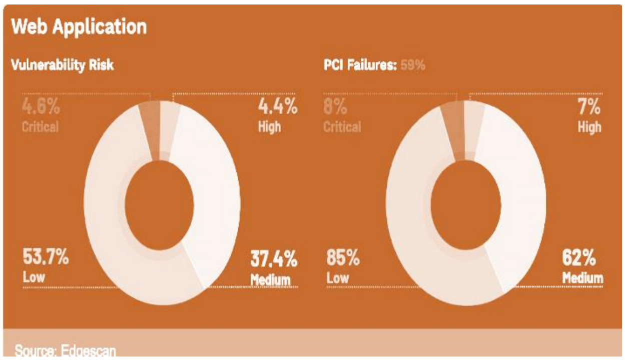

Figure 3: Web application vulnerability risk

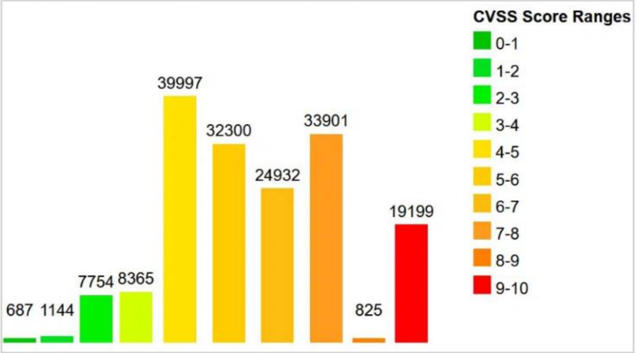

Figure 4: Vulnerability distribution by cvss scores

International statistics showed that at the beginning of the first quarter of 2022, more than 8,000 vulnerabilities were published, representing 8.051% according to the NVD database. If these numbers continue as they are, they represent an increase estimated at 25% compared to the same period of the previous year, as the year 2021 witnessed the publication of More than 22,000 security vulnerabilities are considered half of the vulnerabilities in web applications, according to Edgescan, which analysed the severity of high-risk internal security vulnerabilities in the year 2021. The report included that small companies with a number of employees of less than 100 experienced the lowest number of vulnerabilities compared to medium and large companies, where Companies with more than 10,000 employees saw the largest share of total high-risk vulnerabilities, while mid-sized companies with 101 to 1,000 employees saw the highest percentage of average vulnerabilities. The time it takes to address cyber vulnerabilities, according to Edgescan, is a slight improvement over the year. The average time in the past was 60.3%, while the year 2022 witnessed 57.5%. The data shows that the smaller the institution, the faster it recovers, and vice versa.

VI. RESULTS

This paper contributed to the following results:

1. Vulnerability patching is considered the cheapest tool to protect several platforms and applications, especially financial transactions.
2. The vulnerability practicing could decrease the impact of the attacks to 32%.
3. The vulnerability patching mitigates the cybersecurity threats to 21%.
4. Vulnerability patching Strengthening the security policies of the various institutions,

This work is licensed under Creative Commons Attribution 4.0 International License.

especially the financial ones, and facilitating oversight.

VII. CONCLUSION

This paper is aims to optimized the security posture for the institutions by adapting the damage minimization strategy has proven its effectiveness and feasibility through research and analysis in this study. This algorithm is also characterized by its low cost compared to the rest of the measures. Patching security vulnerabilities has also proven its effectiveness in protecting against various attacks and risks, especially with regard to financial transactions that commonly require more protection.

REFERENCES

[1] Kamal Aldin Yousif. (2019). Networks security assessment of unknown attacks. *IOSR Journal of Computer Engineering (IOSR-JCE), 21*(1), 01-12.

[2] Kamal Aldin Yousif Yaseen. (2019). Networks security models scalability analysis. *Arab Journal of Sciences and Research Publishing (AJSRP), 3*(1).

[3] K. A. Yousif Yaseen. (202). Importance of cybersecurity in the higher education sector 2022. *AJCST, 11*(2), 20–24.

[4] K. A. Yousif Yaseen. (2022). Digital education: The cybersecurity challenges in the online classroom (2019-2020). *AJCST, 11*(2), 33–38.

[5] Huitong Song & Yansheng Chen. (2021). Digital financial transaction security based on blockchain technology. *Journal of Physics: Conference Series*.

[6] Sikorski J J, Haughton J & Kraft M. (2017). Blockchain technology in the chemical industry, machine-to-machine electricity market. *Applied Energy*, *195*(JUN.1), 234-246.

[7] Zhang Y & Wen J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*(4), 983-994.

[8] Benchoufi M & Ravaud P. (2017). Blockchain technology for improving clinical research quality. *Trials, 18*(1), 335.

[9] Qiu, Xue, et al. (2014). An automated method of penetration testing. *Computing, Communications and IT Applications Conference(ComComAp), IEEE*.

[10] Vernotte, Alexandre. (2013). Research questions for model-based vulnerability testing of web applications. *Software Testing, Verification and Validation (ICST), IEEE Sixth International Conference on. IEEE*.

[11] Focardi, Riccardo, Flaminia L. Luccio & Marco Squarcina. (2012). Fast SQL blind injections in high latency networks. *Satellite Telecommunications(ESTEL), IEEE First AESS European Conference*.

[12] Geer, Daniel & John Harthorne. (2002). Penetration testing: Aduet. *Computer Security Applications Conference, Proceedings.18th Annual. IEEE*.

[13] Shao-Ming Tong, Chien-Cheng Huang, Feng-Yu Lin & Yeali Sun. (2016). Patching assignment optimization for security vulnerabilities. *The International Arab Journal of Information Technology, 13*(2).

[14] K. A. Torkura, F. Cheng & C. Meinel. (2015). A proposed framework for proactive vulnerability assessments in cloud deployments. *10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK*, pp. 51-57. DOI: 10.1109/ICITST.2015.7412055.

This work is licensed under Creative Commons Attribution 4.0 International License.