National Vulnerability Database & Common Weakness Enumeration

Ramon Lopez Jr

Department of Cyber Security: University of Advancing Technology

NTS201: Security Essentials

Professor Cameron Miller

October 23rd, 2022

National Vulnerability Database & Common Weakness Enumeration

Vulnerabilities in a network can be classified into distinct categories based on their severity: low, medium, high, or critical. The National Institute of Standards and Technology (NIST) defines vulnerability data as information that "enables automation of vulnerability management, security measurement, and compliance... including databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics" (NIST, n.d.). Identifying which vulnerabilities to patch first is crucial, with high and critical severity vulnerabilities requiring immediate attention.

Common High-Severity Vulnerabilities:

Upon reviewing the NIST database, one of the most commonly identified high-severity vulnerabilities is associated with Jenkins. This vulnerability stems from improper XML parser configurations and the lack of execution limits on agent/controller processes, making it a significant security concern. The NIST database highlights various weaknesses affecting software, hardware, and general security concepts:

- **Software Vulnerabilities**: Open-source software tends to exhibit weaknesses, though most are categorized as low to medium severity.
- **Hardware Vulnerabilities**: A notable high-severity hardware vulnerability is CVE-2021-21348, which allows a remote attacker to occupy a thread that consumes maximum CPU time, rendering the system unresponsive.
- **Concept Weaknesses**: No significant vulnerabilities were identified in the concept category during the review of the NIST database.

Factors Influencing Threat Levels:

Threat levels associated with vulnerabilities can change over time due to several factors. One major influence is the frequency of attacks exploiting a particular vulnerability. According to the National Cyber Security Centre, "[Threat levels] might change if new information emerges that the threat has heightened. This might be because of a temporary uplift in adversary capability, if, for example, there is a zero-day vulnerability in a widely used service that capable threat actors are actively exploiting" (National Cyber Security Centre, n.d.). Updated information on vulnerabilities also contributes to reassessing their severity and potential impact. Both home users and businesses can take initiative-taking measures to mitigate vulnerabilities:

For Home Users:

- **Multi-Factor Authentication (MFA)**: Adds an extra layer of security by requiring additional verification beyond just a password.
- **Software Updates**: Regularly updating software ensures that known vulnerabilities are patched.
- **Strong Passwords**: Using complex and unique passwords reduces the risk of unauthorized access.

For Businesses:

- **Access Control**: Limiting access to sensitive data minimizes human error and insider threats.
- **Network Firewalls**: Implementing firewalls helps prevent employees from accessing malicious or inappropriate websites.

- **Employee Training**: Educating employees about cybersecurity best practices, such as recognizing phishing attempts, significantly reduces security risks.

Relevance of Identified Vulnerabilities:

Upon reviewing the NIST database, none of the listed vulnerabilities pose a direct threat to my systems. Most vulnerabilities are linked to specific applications or software that I do not have installed. For example, the application "Prisma" has a vulnerability where a "custom binary" is executed when VS Code triggers auto-formatting or when validation checks are triggered after each keypress on a *.prisma file" (NIST, n.d.). Since I do not use Prisma, this vulnerability does not affect me. This underscores the importance of contextualizing vulnerabilities based on an individual's or an organization's specific software environment.

Understanding and mitigating vulnerabilities is essential for maintaining strong cybersecurity defenses. By prioritizing high and critical severity vulnerabilities, staying informed on evolving threats, and implementing robust security measures, both individuals and businesses can reduce their risk exposure. This analysis aligns with forensic incident response and digital threat mitigation by emphasizing the identification, assessment, and strategic management of vulnerabilities within cybersecurity frameworks.

References

Ausherman, N. (2019, October 22). *How to Protect Your Business from Cyber Attacks*. NIST. https://www.nist.gov/blogs/manufacturing-innovation-blog/how-protect-your-business-cyber-attacks

Cybersecurity & Infrastructure Security Agency. (n.d.). *4 Things You Can Do To Keep Yourself Cyber Safe | CISA*. Www.cisa.gov. Retrieved October 23, 2022, from https://www.cisa.gov/4-things-you-can-do-keep-yourself-cyber-safe#:~:text=Here%20are%20the%204%20things%20you%20can%20do

National Cyber Security Centre. (n.d.). *Actions to take when the cyber threat is heightened*. Www.ncsc.gov.uk. https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

NIST. (n.d.-a). *NVD - CVE-2021-21415*. Nvd.nist.gov. Retrieved October 23, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2021-21415#vulnDescriptionTitle

NIST. (n.d.-b). *NVD - CVE-2022-43429*. Nvd.nist.gov. Retrieved October 23, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2022-43429

NIST. (n.d.-c). *NVD - CVE-2022-43430*. Nvd.nist.gov. Retrieved October 23, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2022-43430

NIST. (2019). *NVD - Home*. Nist.gov. https://nvd.nist.gov/