WHITE PAPER

Hikvision
Understanding Vulnerabilities

Insights Into the World of Software Vulnerabilities and Vulnerability Management

Contents

HIKVISION®

INTRODUCTION: VULNERABILITIES REMAIN MISUNDERSTOOD

Software vulnerabilities are a reality for everyone who uses technology. Every month, software companies release patches to fix vulnerabilities discovered in the devices we use every day. Windows, MacOS, Linux, iOS and Android all receive patches regularly after new vulnerabilities are discovered in their operating systems. Vulnerabilities are not only limited to operating systems, but software applications, mobile device apps, and even software components are also prone to software bugs, that could give threat actors a foothold into a system. While we all live with the dynamic state of Internet-connected software, vulnerabilities still remain a misunderstood part of our lives.

For simplicity's sake, this paper will address three basic types of software: operating systems, applications/apps, and software components, and firmware. All of these are susceptible to vulnerabilities and will likely have patches released by their respective software vendor, provided the software is supported by that vendor.

1. **Operating System**: Software that manages computer hardware, and resources. Examples are Windows, MacOS, Linux/UNIX, iOS, Android.

2. **Applications/Apps**: Software that runs in an operating system and is used to add functionality and perform specific tasks. Examples are Excel, Google Chrome, Zoom, Adobe Photoshop, Instagram, and Spotify.

3. **Software Components**: Software that is used to add functionality to other software. Often software developers use proven, well-tested software components to add features to their software rather than writing something from scratch. For example, web servers tend to use OpenSSL, the software that gives you the encrypted connection between your browser and the web server. Examples are Log4j and OpenSSL.

So the next time you open a web browser, you are running:

- Browser software *(Chrome, Firefox, Edge, Safari, etc)*
- Software components in that browser *(open source code, plug-ins, etc.)*
- An operating system *(Windows, macOS, Linux)*

Along with the basic types of software, there are also three basic types of computer systems the average person uses or interacts with regularly: workstations, mobile devices, and servers.

1. **Workstation**: A desktop or laptop running an operating system such as Windows, MacOS, or Linux.

2. **Mobile Device**: A smartphone or tablet that runs an operating system like Android or iOS.

3. **Server**: A computer that provides a service over a network like the Internet. Servers also run operating systems like Windows, MacOS and Linux.

All of these computing systems are running software that needs to be updated regularly as new vulnerabilities are discovered and patches are made available by their software vendors. Some of these patches are installed automatically while others require the end-user of the software to install the patches manually. Even when you are up to date with patches, it is likely that you are running vulnerable software but just haven't found all of the vulnerabilities yet.

IoT AND FIRMWARE

In addition to the traditional computing device that we use every day, there is a large and growing family of computers that many people forget about when building a cybersecurity strategy. Internet of Things (IoT) devices are systems that were traditionally used in the kinetic world, but were given Internet connectivity to add features or convenience. These "smart" systems, like IP video security cameras, smart thermostats, and smart appliances typically run on firmware, which is a method of embedding an operating system and software into hardware.

A specific kind of software that is typically embedded in hardware. Many IoT devices have an operating system and applications embedded in their firmware. Unlike regular software patching, where a small piece of flawed code can be replaced with its respective patched code, firmware requires a full replacement of the old firmware with the new firmware.

WHAT ARE VULNERABILITIES?

The U.S. Department of Commerce National Institute of Standards and Technology Computer Security Resource Center defines a vulnerability as a security flaw, glitch, or weakness found in software code that could be exploited by an attacker — with an attacker being the source of the threat. Essentially, a vulnerability is a weakness in code that when exploited, has a negative impact on confidentiality, integrity or availability. While some vulnerabilities are more severe than others, it is important to base vulnerability mitigation efforts on severity and risk.

WHAT IS A RISK?

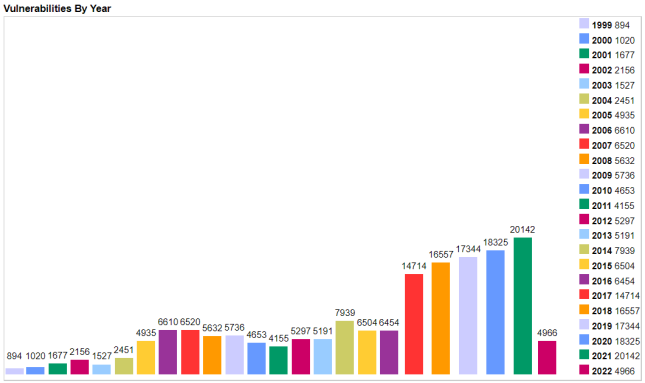
A cybersecurity risk is the probability that a vulnerability will be exploited by a threat actor. To use a real-world example, leaving your front door unlocked is a vulnerability. However, the risk that a threat actor would try to enter the unlocked door of your house is much greater in a heavily populated city than it is for a house on a remote island in Iceland. Similarly, in the digital world an Internet-accessible computer will be scanned and attacked every day so patching known vulnerabilities on those systems in a timely manner is critically important. However, if that same system were placed on an isolated network where only trusted users have physical and logical access, the risk of attack is negligible so the urgency to patch is much lower.

HOW ARE VULNERABILITIES DISCOVERED?

The number of vulnerabilities being disclosed annually has increased every year since 2016. In 2020, more than 20,000 vulnerabilities were publicly disclosed. That averages to more than 55 vulnerabilities being disclosed every single day. So, how are these vulnerabilities being discovered so frequently?

Vulnerabilities are often discovered in software through a few different avenues — both internally, by the software developers who made the software, and externally by third parties who look for vulnerabilities in software.

Internally, responsible software companies will conduct security testing during the software development life-cycle before putting software into production and making it available to the public. They will also continue to test their software after it is put into production so they can identify vulnerabilities by using updated security tools and methods.



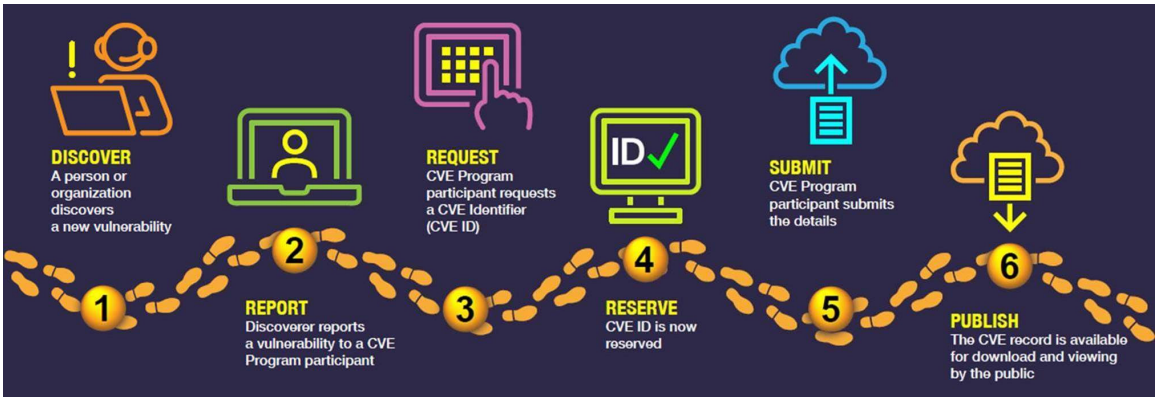
Externally, malicious threat actors and ethical security researchers are constantly looking for vulnerabilities in popular software. Malicious threat actors look for vulnerabilities so they can exploit those vulnerabilities in other people's computer systems, or sell the information to another threat actor. Security researchers look for vulnerabilities in order to have them fixed. Typically, when a security researcher discovers a vulnerability in a product, they will alert the software vendor who owns and manages that product and work with the vendor to identify the vulnerability, create a patch, and test it to ensure that the patch fixes the vulnerability. Some software vendors have a formal bug bounty program, where they reward researchers for responsibly disclosing vulnerabilities with the vendor. These rewards can range in value from vendor-branded logo gear to a cash reward.

HOW ARE VULNERABILITIES DISCLOSED?

The question of when to publicly disclose a vulnerability is a controversial topic because there are a lot of factors to take into consideration, but the main goal is to reduce the risk of end users' systems becoming compromised by a threat actor who exploits an unpatched vulnerability.

If a security researcher and a software vendor work together, following a coordinated disclosure process, both entities will not let the public know of the vulnerability until a working patch is made available. The reason for this is because as soon as threat actors know that a vulnerability exists in a product, many will aggressively look for that vulnerability in order to exploit it before the patch is released.

On an agreed upon disclosure date, the vendor will release the patch and make a public statement that a vulnerability was discovered and a patch has been released. The researcher will likely make a public statement as well, taking credit for discovering the vulnerability and working with the software vendor. This is also the point at which an entry into the Common Vulnerabilities and Exposures (CVE) database will be made. If the vendor or the researcher is a CVE CNA, they can issue the CVE themselves, if not, they will need to report the vulnerability to a CVE Program participant. The process for submitting a CVE is outlined on the CVE website and in the following image.



Copyright © 1999-2022, The MITRE Corporation

HOW ARE VULNERABILITIES MANAGED?

With the continual emergence of digital attacks, organizations are under constant pressure to identify and mitigate threats in a timely manner. Unfortunately, many IT departments do not have the resources necessary to effectively identify vulnerabilities and quickly install the patches needed to safeguard their systems. As such, many organizations are hiring contract workers to assist with the rapidly growing number of patches that are released every month.

For organizations to protect themselves from cyber-attacks that leverage known vulnerabilities, they can implement a risk-based vulnerability management process. Even a small organization with only a few computers and devices can benefit from an established process that assesses risks and prioritizes patching and mitigation based on the level of risk.

Some large organizations have ethical hackers or penetration testers on staff who are looking for vulnerabilities in their enterprise, but for organizations who don't have the budget for this, here are a few key tools and references that can be used to properly manage vulnerabilities in an organization.

VULNERABILITY MANAGEMENT TOOLS AND REFERENCES

Vulnerability Scanners

Vulnerability scanners search networks for systems that have known vulnerabilities and help identify the severity of vulnerabilities detected, a great first step to beginning vulnerability management. Some vulnerability scanners come with additional tools that assist organizations in managing and remediating vulnerabilities. Some popular commercial and open-source tools are listed below.

- Nessus by Tenable®
- Qualys® VMDR
- InsightVM
- Burpsuite
- OpenSCAP Vulnerability Assessment
- OpenVAS

Common Vulnerabilities and Exposures (CVE) Database

The Common Vulnerabilities and Exposures (CVE) database is the de facto standard for identifying and referencing known vulnerabilities. The MITRE Corporation launched the CVE database in 1999 with the goal of identifying, defining, and cataloging publicly disclosed vulnerabilities.

Over the years, MITRE began to partner with organizations who help manage the database. Originally known as CVE Numbering Authorities (CVE CNA), these organizations are now known as CVE Partners. As of the writing of this white paper, there are more than 225 CVE partner organizations around the world. These are organizations that manage the globally recognized CVE database, founded by the MITRE Corporation in the suburbs of Washington, D.C.

National Vulnerability Database (NVD)

In addition to identifying vulnerabilities, it is also important to also assess their severity. With the sheer number of vulnerabilities every day, it is important to know which to address first. The National Institute of Standards and Technology (NIST) manages the National Vulnerability Database (NVD), which scores the severity of vulnerabilities. The NVD supports both Common Vulnerability Scoring System (CVSS) v2.0 and v3.X standards.

Table 1. CVSS Qualitative Severity Rating Scale

CVSS Score	Severity Rating
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

The CVSS provides a standardized vulnerability scoring method that assists organizations in prioritizing their vulnerability mitigation efforts. Using this scoring system, vulnerabilities are categorized into one of five ratings based on the vulnerability assessment score. The scores range from zero (no severity) to 10 (critical severity). A table of the scoring scale is shown in Table 1.

One thing to note, is that the NVD does not, and cannot provide an environmental score, which indicates how that vulnerability impacts your environment. So, it is recommended that the NVD CVSS score be used as a baseline, but organizations should recast CVSS scores based on their environmental risks.

Recasting CVSS Scoring for You

As mentioned earlier, a locked door in a city is far more necessary than one on a remote island. Similarly, a vulnerable Internet-accessible system should be patched immediately while a similar system with strong network security controls may be mitigated at a lesser priority. Organizations can use the CVSS calculator to calculate a temporal and environmental score and receive a more accurate security score and assessment of risk.

The environmental score is used to assess the risk of a particular system that is running vulnerable software. For example, if an organization has a web server on the Internet, and an exact copy of that web server in a controlled development lab, the organization would create an environmental score for each of those web servers. Obviously, the web server that is Internet-accessible would have a much higher score than the one in the lab, therefore the web server on the Internet would be patched more urgently than the web server in the lab.

The temporal score is used to assess risk based on a few factors, including whether attackers are actively exploiting the vulnerability in the wild and if there is a patch or workaround available to mitigate the vulnerability. This section can be difficult for organizations to fill out because exploit information can change day to day and is not easily accessible to the general public. One alternative is to reference CISA's Known Exploited Vulnerabilities Catalog.

CISA's Known Exploited Vulnerabilities Catalog

Now that you have a vulnerability scanner to identify known vulnerabilities on your systems, and you understand how to recast a severity score to reflect the risk of those vulnerabilities in your environment, it's time to learn how to prioritize your vulnerability management efforts based on real-world threats.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) determined that CVSS scores do not always accurately depict the threat a CVE presents.

> *Many attackers do not rely only on "critical" vulnerabilities to achieve their goals; some of the most widespread and devastating attacks have included multiple vulnerabilities rated "high," "medium," or even "low."*

CISA also reports that many "critical" vulnerabilities are highly complex and have never been seen exploited in the wild—in fact, only 4% of the total number of CVEs have been publicly exploited. However, threat actors are extremely fast to exploit new vulnerabilities. Of those 4% known exploited CVEs:

- 42% are being exploited on day 0 of disclosure
- 50% within 2 days
- 75% within 28 days

So, it is critically important to patch vulnerable and exposed systems as soon as possible. Based on this research, CISA changed the strategy of vulnerability management for U.S. federal agencies in November 2021. Instead of only focusing on vulnerabilities that carry a specific CVSS score, CISA is targeting vulnerabilities for remediation that have known exploits and are being actively exploited by malicious cyber actors.

To date, there are more than 700 vulnerabilities listed in CISA's Known Exploited Vulnerabilities Catalog and it is updated regularly as CISA identifies more exploited vulnerabilities. If you find these vulnerabilities on your systems, they should be prioritized for remediation.

Vulnerability Management Lifecycle

The U.S. Department of Defense developed a timeline for their Vulnerability Disclosure Program (VDP). It includes five stages, from the "discovery" of a vulnerability, to "lessons learned."

Stage 1: Discovery
The discovery of a vulnerability occurs when software is found to have an exploitable flaw. If the vulnerability is discovered because it is being actively exploited, it is referred to as a "0-day" (zero day) vulnerability.

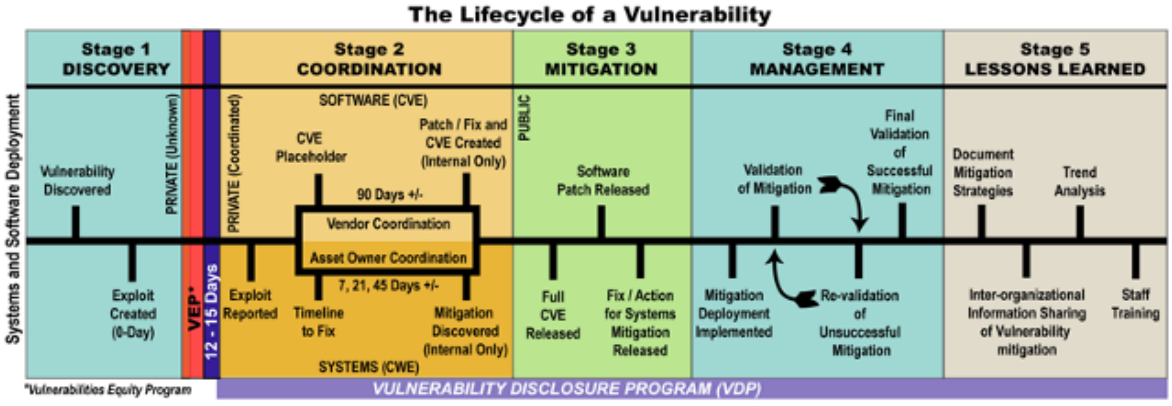
Stage 2: Coordination
During the coordination stage, the existence of the vulnerability is verified and a plan is put in place to mitigate the vulnerability. At this point, a CVE may be created as a placeholder with no details.

Stage 3: Mitigation
Mitigation includes the release of a patch or work-around and the publication of a full CVE.

Stage 4: Management
Once the mitigation has been publicized, end users of the vulnerable software need to install the patches or apply the work-arounds and verify that the vulnerability has been mitigated.

Stage 5: Lessons Learned
The last stage is to review document mitigation strategies, review mitigation efforts across organizations, and analyze trends. Then, identify if there are ways to better respond to similar vulnerabilities in the future.

The Lifecycle of a Vulnerability timeline identifies responsibilities to be executed by a few different roles. Organizations who are managing vulnerabilities need to understand the whole process but focus on creating repeatable processes in the management and lessons learned stages.



Roles & Responsibility

Cybersecurity is everyone's responsibility and understanding one's role is important in protecting computer systems and the Internet at large. The basic roles and responsibilities in vulnerability management are outlined below.

Security Researcher
Security researchers are an important part of the vulnerability management ecosystem. They use their skills and tools to find vulnerabilities in software and work with software vendors to ensure that patches or other remediation solutions are made available to end users. Security researchers should be careful when they publicly disclose information and should work with the software vendor to coordinate their disclosures in a strategic manner that best protects the end users.

Software Vendor
Software vendors have three basic responsibilities.

1. Secure: Build security into products. This means ensuring that code reviews and vulnerability scanners are used throughout the software development life-cycle.
2. Respond: Be ready to respond to the discovery of vulnerabilities in their products. Have a Product Security Incident Response Team (PSIRT) ready to work with security researchers or respond quickly to the discovery of a 0-day vulnerability in their software.
3. Communicate: Ensure that patching and remediation solutions are quickly and clearly communicated to customers and the public.

End Users
End users have two basic responsibilities.

1. Network Security: Systems should be placed behind firewalls and remote access should be limited to more secure methods, such as using VPNs rather than making systems directly accessible from the Internet. Networks should also be segmented to access the systems given to only those who have a need. Attackers can't exploit vulnerabilities if they can't reach them.
2. System Security: A few basic cybersecurity best practices go a long way in preventing successful cyberattacks.

    a. Create strong passwords/use a password manager
    b. Use multi-factor authentication wherever possible
    c. Patch your systems quickly and regularly

CONCLUSION

The number of vulnerabilities that exist in devices, networks, and applications has only continued to grow, particularly as technology continues to evolve and our lives become more interconnected. CISA states that without a clear understanding of an organization's Internet-accessible footprint, it is not only difficult to identify anomalies, risks, and misconfigurations, but it is also impossible to defend against what one does not know. In order to build and maintain a vulnerability management program, it is helpful to understand the lifecycle of a vulnerability and what options are available for businesses to help mitigate those risks. A vulnerability management program helps to ensure that an organization maintains a comprehensive understanding of its critical services and meets its responsibility to its stakeholders, while contributing to security of the Internet at large.

It is critical for all companies to put cybersecurity issues at the forefront and prioritize standing up a robust vulnerability management program within the organization.

REFERENCES

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Nature of the Computer Security Community.* Cyber Threat Source Descriptions | CISA.
https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Reducing the Significant Risk of Known Exploited Vulnerabilities.* Reducing the Significant Risk of Known Exploited Vulnerabilities.
https://www.cisa.gov/known-exploited-vulnerabilities

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.-c). *What is the Vulnerability Management (VULN) Security Capability?* Vulnerability Management FAQ.
https://www.cisa.gov/uscert/cdm/capabilities/vuln

Cybersecurity and Infrastructure Security Agency (CISA). (2022, January). *CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems.*
https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2016). *CRR Supplemental Resource Guide, Volume 4: Vulnerability Management.*
https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf

Common Vulnerabilities and Exposures (CVE). (2022). *CVE Process.*
Copyright © 1999-2022, The MITRE Corporation.
https://www.cve.org/About/Process

Common Vulnerabilities and Exposures (CVE). (2022). *CVE Homepage.*
Copyright © 1999-2022, The MITRE Corporation.
https://cve.mitre.org/index.html

Common Vulnerabilities and Exposures (CVE). (2022). *CVE List of Partners.*
Copyright © 1999-2022, The MITRE Corporation.
https://www.cve.org/PartnerInformation/ListOfPartners

D. Votipka, R. Stevens, E. Redmiles, J. Hu and M. Mazurek. (2018). "Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes." *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 374-391, doi: 10.1109/SP.2018.00003.

History of Yesterday. (2021). *The Story Behind a Lone House in the Middle of Elliðaey Island.* https://historyofyesterday.com/the-story-behind-a-lone-house-in-the-middle-of-elli%C3%B0aey-island-529309b9cc22

National Institute of Standards and Technology (NIST). (n.d.). *CVSS Score Distribution for Top 50 Vendors by Total Number of Distinct Vulnerabilities.* CVE Details. https://www.cvedetails.com/top-50-vendor-cvssscore-distribution.php

National Institute of Standards and Technology (NIST). (n.d.). NVD - *Full Listing.* National Vulnerability Database Full Listing. https://nvd.nist.gov/vuln/full-listing

National Institute of Standards and Technology (NIST). (n.d.). *Software Vulnerability - Glossary | CSRC.* Computer Security Resource Center Glossary. https://csrc.nist.gov/glossary/term/software_vulnerability

National Institute of Standards and Technology (NIST). (n.d.). *Zero Day Attack - Glossary | CSRC.* Computer Security Resource Center Glossary. https://csrc.nist.gov/glossary/term/zero_day_attack

Hikvision USA Inc.
18639 Railroad Street
City of Industry, CA 91748

Hikvision Canada Inc.
4848 Levy Street
Saint-Laurent, Quebec H4R 2P1

Contact Information
Toll-Free: +1 866-200-6690 (U.S. and Canada)
Phone: +1 909-895-0400
Email: sales.usa@hikvision.com
hikvision.com

Connect with us:

HIKVISION®