NETRISE

Supply Chain Visibility & Risk Study

Edition 1: Networking Equipment; Q3 2024

Executive Summary: Overview and Key Findings

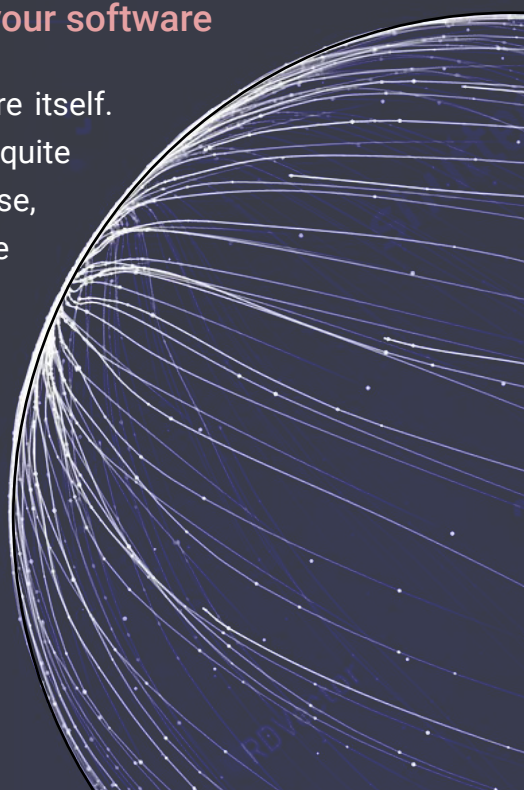
All companies rely on software to power their business. However, software development pressures and the corresponding enterprise software sprawl is driving up software supply chain risks. These risks are much greater than most security professionals understand. In fact, the software risk data most rely on today is only the tip of the iceberg and misses many of what should be considered the highest priority software risks that exist in the enterprise.

However, we see that understanding the true software supply chain risks starts with building a detailed inventory and control of software assets (including a full SBOM of all the software components) which organizations struggle with today. According to Sonatype's ninth annual State of the Software Supply Chain report, the supply chain of open source and proprietary libraries is so complex that only 7% of organizations interviewed have even attempted to review their supply chain risks.[1]

Key Findings and Recommendations

1 | To understand software risks, start with an inventory of your software

- Understanding software risks starts with visibility into the software itself. Every piece of software, no matter how reputable the source, is quite complex and poses risks. It's critical that those who build, buy, use, and maintain the software can inventory and understand the scope and scale of their software. A deep analysis of the software using a compiled and interpreted code analysis is one way to get to this information.
- Using this analysis approach, we generated detailed SBOMs for the tested networking equipment and saw that each device contains 1,267 software components on average.



netrise.io | sales@netrise.io

2 | Identifying software risks requires a new approach and new data

- We find that the vulnerability risks are on average 200 times greater for the 5 networking equipment asset classes covered in this study than what traditional network-based vulnerability scanners would lead one to believe.
- We find that the average network equipment device has 1,120 known vulnerabilities in the underlying software components, with over 1/3 of them being more than 5 years old and some even more than 10 years old.

Unidentified software risks are 200 times greater than what is commonly understood.

3 | To prioritize software risks, stop relying solely on CVSS Severity Scores

- Using the detailed software analysis in this research, we find that of the average 1,120 known vulnerabilities per networking device, 42.3% are ranked Critical or High per the CVSS Severity scores. That's 473 critical and high vulnerabilities per networking device - more than any team can reasonably expect to respond to.
- Instead, we find that there are only 20 weaponized vulnerabilities per networking device on average. And looking closer there are only 7 weaponized vulnerabilities that are also network accessible. Using this approach, we find a much more reasonable number of vulnerabilities that we might need to address.

Introduction and Purpose

Introduction - Trust But Verify

All companies rely on software to power their business, to connect with customers and partners, to automate back-office processes, and to build market presence. Today's world is built on software – 3rd party software, open source software, in-house developed software, operating system software, applications, containers, and device firmware to name a few.

Developers are tasked with building the business-critical software we use everyday and they face continuous pressure to release value to customers faster than ever before. This development pressure and the corresponding enterprise software sprawl creates a growing software supply chain visibility and risk challenge.

However, this reliance on software comes with a hidden danger: the blind trust placed in the software. Many companies assume that the software they purchase is secure and free from vulnerabilities and risks, but recent high-profile software supply chain breaches have proven otherwise. The reality is that every piece of software, no matter how reputable the source, poses risks.

This is where the principle of "trust but verify" becomes crucial. Blind trust in software can lead to devastating consequences, from data breaches to operational disruptions. Comprehensive visibility into all software components and dependencies is an essential starting point for software supply chain security.

Comprehensive visibility into all software components and dependencies is an essential starting point for software supply chain security.

Cyber adversaries know there is a growing software supply chain visibility and risk challenge. In fact, software supply chain attacks have seen triple-digit increases, but far too few organizations have taken steps to evaluate the risks of these complex attacks in their software supply chain.

According to Capterra's "2023 Software Supply Chain Survey", 61% of companies have been impacted by a software supply chain cyber attack in the 12 months prior to the survey.[2] In fact, current research shows software supply chain attacks are a global challenge that continues to grow dramatically.[1,2] Despite this, proactive efforts to identify, assess and mitigate software supply chain risks are relatively rare. Only 7% of respondents to Sonatype's ninth annual State of the Software Supply Chain report have made efforts to review security risks in their supply chains.[1]

According to Capterra's "2023 Software Supply Chain Survey", 61% of companies have been impacted by a software supply chain cyber attack in the 12 months prior to the survey.

Purpose

The purpose of this NetRise "Software Supply Chain Visibility & Risk Study" is to get beyond the marketing reports and state of the market reports, and look at actual software compositions, vulnerability risks, and non-CVE risks that exist in different asset classes that are in every business's software supply chain. The objective is to educate and inspire CISOs, security professionals, and procurement teams to understand the scope and scale of software and software risks that likely exist within their software supply chains and to take proactive steps to securing their software supply chains.

The objective is to educate and inspire CISOs, security professionals, and procurement teams to understand the scope and scale of software and software risks that likely exist within their software supply chains and to take proactive steps to securing their software supply chains.

Scope and Methodology

Research Scope

Recent research by ForeScout has highlighted that network equipment has now surpassed traditional endpoints (laptops, desktops, and servers) to become the riskiest IT device category in 2024.[3]

With that backdrop, this NetRise "Software Supply Chain Visibility & Risk Study" looks at the asset class of networking equipment, specifically, focusing on five classes:

1. **Routers**
2. **Switches**
3. **Firewalls**
4. **Virtual Private Network (VPN) Gateways**
5. **Wireless Access Points**

Each class represents a vital component of the enterprise network, and vulnerabilities within these devices can have far-reaching consequences. The scope of this research includes a comprehensive analysis of the software embedded in these devices, leveraging the leading compiled code analysis capabilities of the NetRise Platform.

By analyzing the software and reporting on the vulnerabilities and risks associated with key networking equipment, this report hopes to underscore the urgent need to prioritize software supply chain security.

Network equipment forms the backbone of enterprise IT infrastructure, enabling connectivity, communication, and access to critical resources. However, this very interconnectedness also makes it a prime target for cyber attackers. According to ForeScout's recent report, network infrastructure devices such as routers and wireless access points are frequently exploited due to their exposure online and dangerous open ports. The report reveals that attackers are increasingly targeting these devices, finding new vulnerabilities and exploiting them in large-scale campaigns.

The report goes on to state that they see a reversal which represents an increase in the number of vulnerabilities found and exploited in network infrastructure devices since the second half of 2023.

Research Methodology

The research methodology employed for this report is designed to provide a detailed and holistic understanding of the software risks associated with each class of networking equipment. The following steps outline the research process:

1. **Software Bill of Materials (SBOM) Analysis:**
   Objective: Gain complete visibility into the components that constitute the software running on each device.
   Process: Use the NetRise Platform to generate detailed SBOMs for each device class. This involves identifying all software components, including third-party libraries and dependencies, to understand the complete software stack.

2. **Vulnerability and Non-CVE Risk Assessment:**
   Objective: Evaluate the risk state of each device, considering both known vulnerabilities (CVEs) and non-CVE risks.
   Process: Use the NetRise Platform to identify vulnerabilities listed in the CVE database, and non-CVE risks, such as misconfigurations, outdated components, and potential security flaws that are not yet publicly disclosed.

3. **Comparison with Traditional Network Based Vulnerability Scanning:**
   Objective: Benchmark the findings from the NetRise Platform against results obtained from traditional vulnerability scanning methods.
   Process: Traditional vulnerability scanners and NVD results are used as a baseline to compare the comprehensive risk assessments provided by the NetRise Platform. This comparison highlights discrepancies and underscores the urgent need for an ‘inside-out’, thorough SBOM-based analysis approach.

Current State of the Market

Market Research and Statistics

Security teams struggle to respond to vulnerabilities, especially where that vulnerability is included within embedded software dependencies. Because software components have not been traditionally

disclosed, their content is often opaque to teams trying to ascertain whether they are affected. This requires extraordinary work to identify affected software and implement risk mitigations.

According to a recent Ponemon study, only 29% of organizations are conducting post-build software dependency/artifact analysis to prevent malicious packages from impacting the software they build, buy, or use.[4] And only 38% of respondents say budget and staffing dedicated to securing the software supply chain is sufficient or very sufficient.[4]

The lack of transparency and trust within the global software supply chain has emerged as a critical issue for organizations. It's well understood that modern application development increasingly relies on open-source and, sometimes, commercially licensed third-party libraries. Thus, transparency into the contents of commercial software is essential to properly evaluate and vet the contents of the software against organizational standards for supply chain and operational risks. The presence of unremediated or unmitigated vulnerabilities within the code leaves organizations open to:

- **The presence of unknown software risks** in the form of unremediated and/or unmitigated vulnerabilities within the organization's software supply chain.
- **Potential legal risks** resulting from onerous or unattractive licensing terms and conditions associated with dependencies that may be inherited by the ultimate end user of the application.
- **Operational and supply chain risks** including factors such as the presence of significant technical debt in licensed software or software lacking appropriate security controls and checks.

The transparency required to effectively address and avoid such issues starts with the SBOM. In its most basic form, and like other bills of materials, SBOMs list the individual software components — open source, commercial, and (in some cases) proprietary — utilized in the creation of a piece of software. But while SBOMs are considered a best practice and critical to having a secure software supply chain, only 35% of respondents say their organizations produce or generate SBOMs.[4]

Within some industry segments, robust approaches to the use and management of SBOMs have already emerged. Examples of these groups tend to be segments where regulatory mandates have driven the adoption of SBOMs, such as medical devices or automobile manufacturing.[4]

Lastly, a detailed understanding of the software within an organization, can be critical to timely cyber attack investigation, response, and remediation. But only 38% of organizations say they are very or highly effective in detecting and responding to an attack on a software vulnerability. And almost half (47%) say it takes at least a month to more than 6 months to respond to a critical software vulnerability.

Market Trends

The industry is however, beginning to make progress in software supply chain security and risk management. This progress is being driven by several factors, including:

Increasing Software Supply Chain Cyber Threats
Networking devices such as routers, switches, firewalls, VPN gateways, and wireless access points have become prime targets for cyber attackers. As noted earlier, they are now considered the riskiest IT device category, surpassing traditional endpoints. And attackers are exploiting vulnerabilities in these devices at an alarming rate, often using them as entry points for broader network compromises.

Further, the proliferation of XIoT devices has significantly expanded the attack surface. IoT vulnerabilities have increased by 136% from the previous year, underscoring the need for comprehensive security measures across all connected devices.

Regulatory and Compliance Pressures
Governments and regulatory bodies are implementing stricter regulations to ensure the security of networking equipment and connected devices. Compliance with standards such as the National Institute of Standards and Technology (NIST) guidelines and the European Union's General Data Protection Regulation (GDPR) is becoming mandatory for many organizations. There is also a growing emphasis on the use of SBOMs to enhance transparency and security.

Technological Advancements
Organizations are increasingly adopting advanced software supply chain analysis and security tools for advanced risk management programs. These security tools provide:

- Detailed SBOM development for all software including embedded firmware, operating systems, virtualization software, and applications.
- Detection of vulnerabilities and non-CVE risks associated with all of the SBOM software components in use.
- Prioritization of all identified software supply chain risks.

Information from these tools can then enrich and feed asset discovery and management tools and intrusion detection tools used within security operations.

Research Data

Software Bills of Materials Analysis for the 5 Classes of Networking Equipment

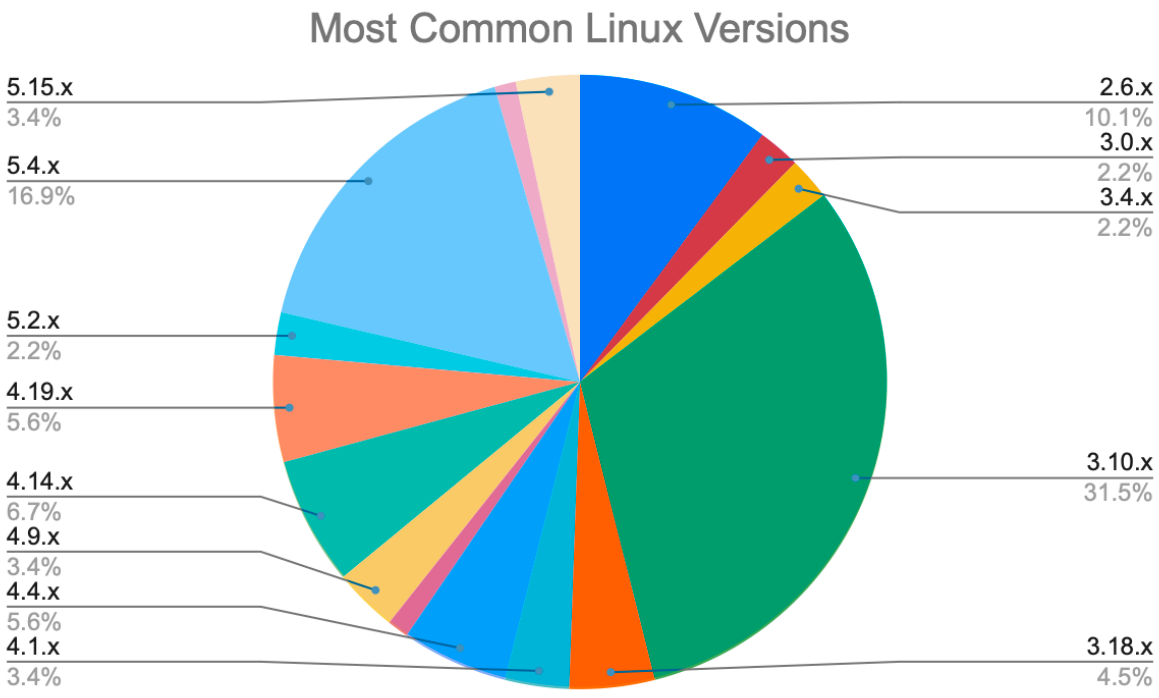
Below we look at a summary of the software analysis for the 100 networking equipment devices analyzed. We look at the number of software components per device, the different versions of Linux Kernels in use, and the number of different versions of some of the most common components in use.

Average Number of Software Components per Networking Device

For the 100 networking devices analyzed, each networking device had on average 1,267 software components.

Linux Kernel Software in Use

For the 100 networking devices analyzed, there were 15 different major versions of Linux Kernels in use and a total of 45 different versions of Linux Kernel in use (listed below).



45 Versions of Linux Kernels

Name	Version
linux_kernel	2.6.30.9
linux_kernel	2.6.32.59
linux_kernel	2.6.32.68
linux_kernel	2.6.36
linux_kernel	2.6.36.4

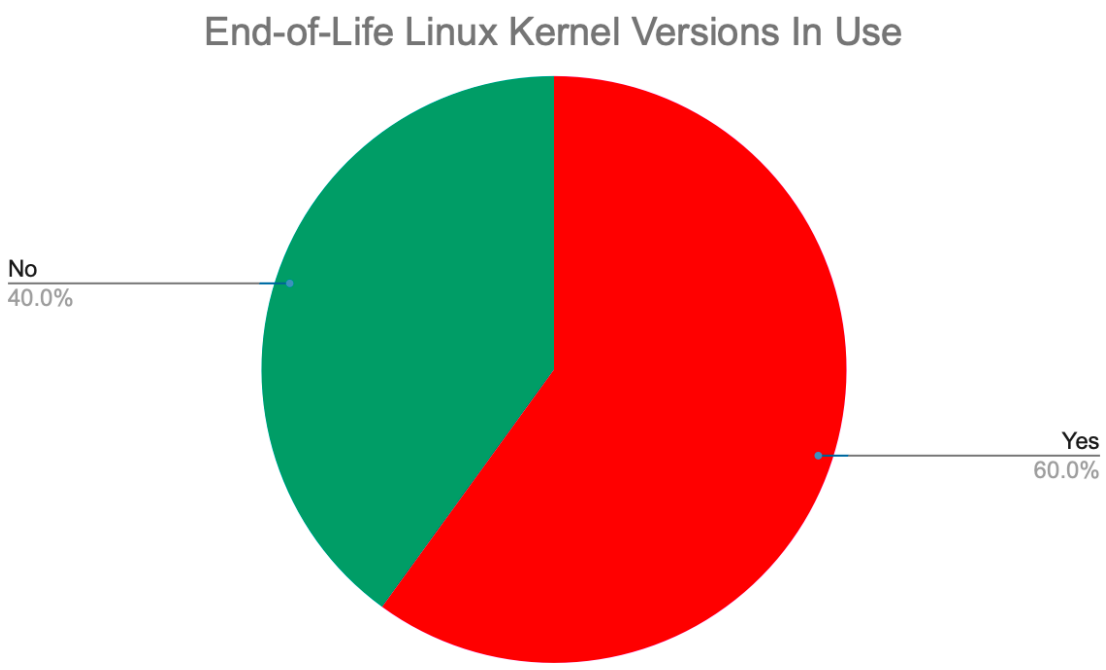
Name	Version
linux_kernel	3.0.31
linux_kernel	3.4.11
linux_kernel	3.4.110
linux_kernel	3.10.0
linux_kernel	3.10.101
linux_kernel	3.10.55
linux_kernel	3.10.62
linux_kernel	3.18.21
linux_kernel	3.18.24

Name	Version
linux_kernel	4.1.27
linux_kernel	4.1.52
linux_kernel	4.4.115
linux_kernel	4.4.120
linux_kernel	4.4.302
linux_kernel	4.8.28
linux_kernel	4.9.187
linux_kernel	4.9.314
linux_kernel	4.9.79
linux_kernel	4.14.0
linux_kernel	4.14.101
linux_kernel	4.14.117
linux_kernel	4.14.254
linux_kernel	4.14.4
linux_kernel	4.19.152

Name	Version
linux_kernel	5.2.60
linux_kernel	5.4.155
linux_kernel	5.4.159
linux_kernel	5.4.164
linux_kernel	5.4.212
linux_kernel	5.4.213
linux_kernel	5.4.216
linux_kernel	5.4.231
linux_kernel	5.4.241
linux_kernel	5.4.74
linux_kernel	5.10.0
linux_kernel	5.15.0
linux_kernel	5.15.111

Active End Of Life

Of the 45 different Linux Kernel versions in use, 60% are currently end-of-life.



Software Components and Versions

For the 100 networking devices analyzed, there were 22,637 different software components, and if we look at unique versions of those components then we find 35,683 unique software components/versions. And some of the most common component types are listed in the table below showing how many different versions of each exist.

Component Name	Unique Version
libcurl	40
libexpat	19
module-init-tools	50
openssl	51
zlib	16

Vulnerability and Non-CVE Risk Assessment Analysis for the 5 Classes of Networking Equipment

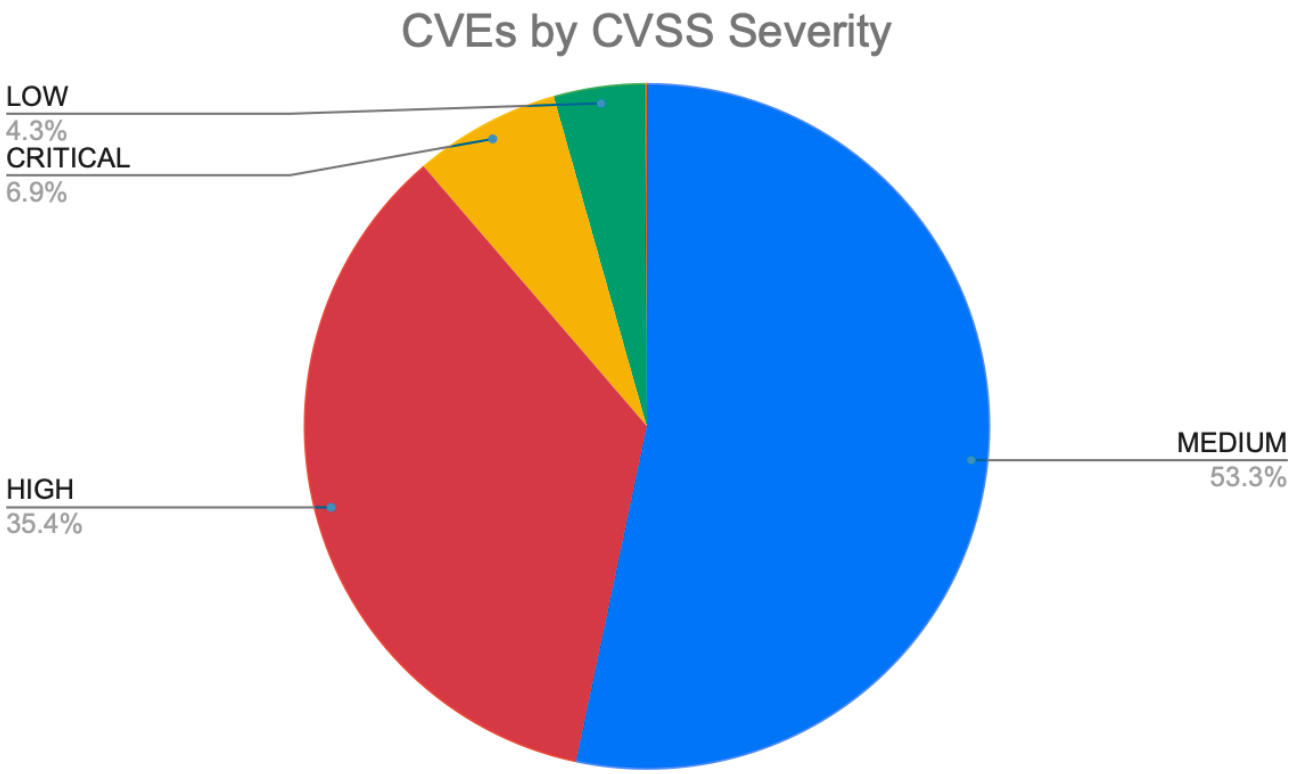
Below we look at a summary of the vulnerability analysis for the 100 networking equipment devices analyzed. We look at the number of CVEs per networking device, the CVE CVSS scores, the number of weaponized and network accessible vulnerabilities, and the age of different CVEs.

Average Number of CVEs per Networking Device

For the 100 networking devices analyzed, each networking device had on average 1,120 CVEs. There were 112,026 total CVEs found in the 100 devices. And there are a total of 4,862 unique CVEs found across the 100 devices.

CVEs by CVSS Severity

Of the 112,026 identified CVEs, 42.3% ranked Critical or High per the CVSS Severity scores.

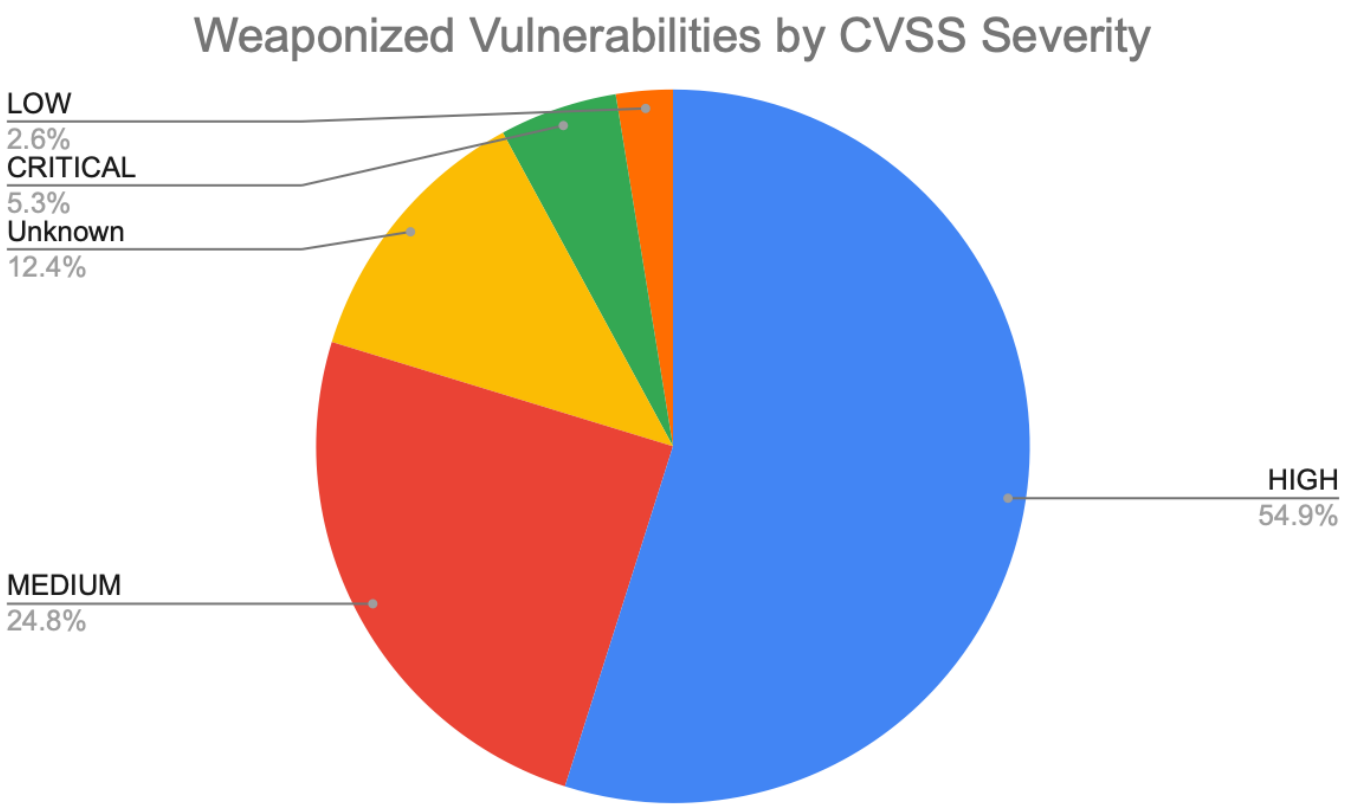


Weaponized Vulnerabilities (Total and by CVSS Severity)

Of the 112,026 identified CVEs, 2,022 (or 1.8%) were found to be weaponized vulnerabilities per NetRise's threat intelligence.

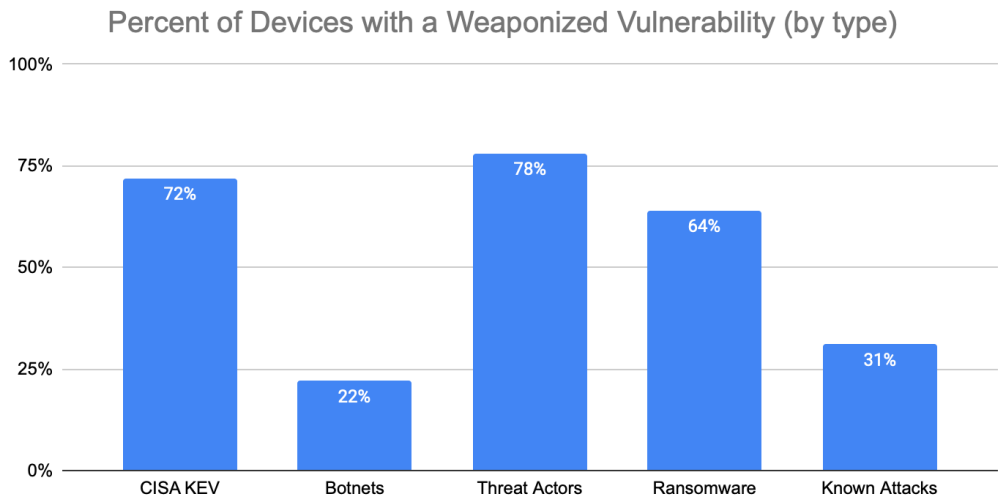
"Weaponized vulnerabilities" as a category include vulnerabilities present in the CISA KEV catalog, those known to be used by botnets, to spread ransomware, used by threat actors, or used in known attacks.

Most interesting is that the vast majority of weaponized vulnerabilities are High and Medium CVSS Severities, not Critical. This is the primary reason NetRise suggests not solely relying on CVSS Severity to drive patch management and supply chain detection and response efforts.



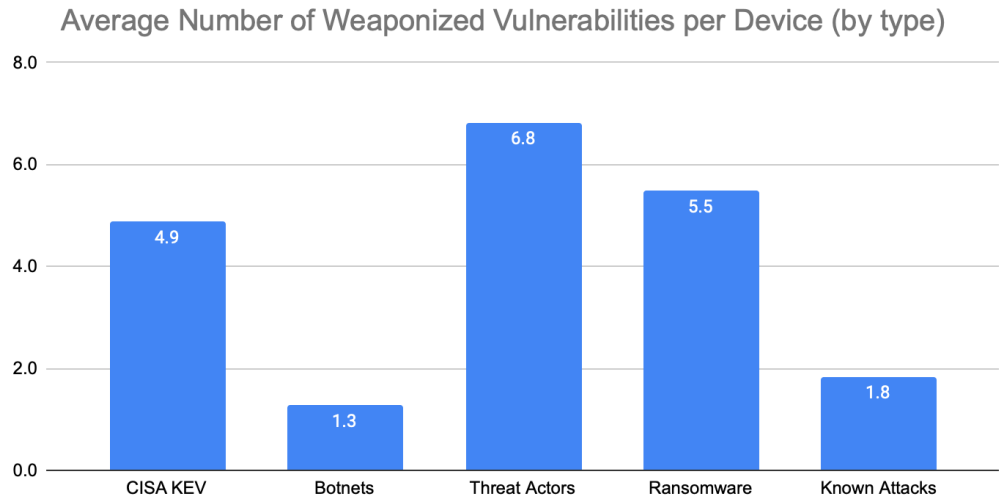
Networking Equipment with Weaponized Vulnerabilities

Seventy two percent (72%) of the 100 networking equipment devices analyzed had at least one vulnerability that is on the CISA KEV. Further, 22% had vulnerabilities used by botnets, 78% had vulnerabilities used by known threat actors, 64% had vulnerabilities known to be used for spreading ransomware, and 31% had vulnerabilities known to be used in other attacks.



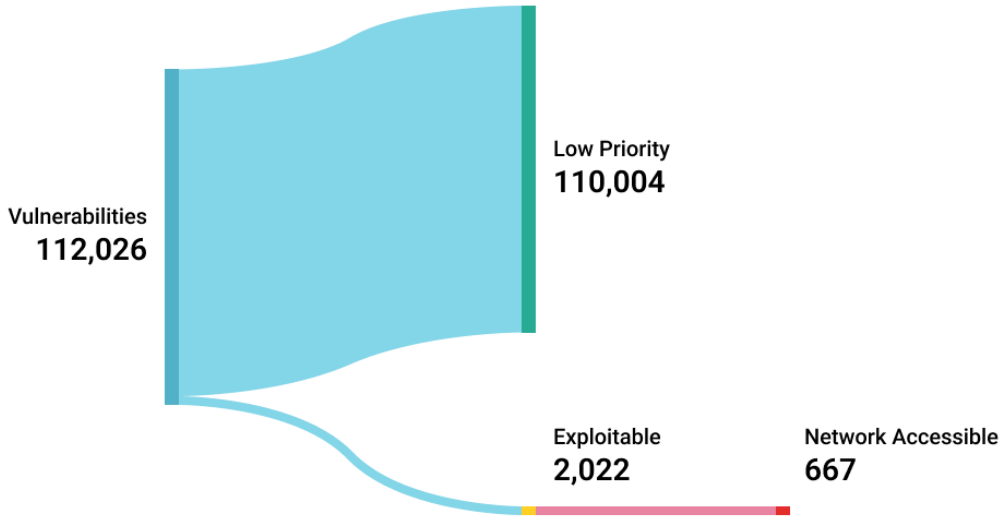
Further, if we look at the average number of weaponized vulnerabilities per each of the 100 networking equipment devices, we find that there are almost five (4.9) CISA KEV vulnerabilities per device. Other types of weaponized vulnerabilities per device are also listed.

The weaponized vulnerability metric is an important threat source because it can be used to identify what known exploitable vulnerabilities exist within the environment which provides a focused list on where to prioritize remediation efforts.



Network Accessible Weaponized Vulnerabilities

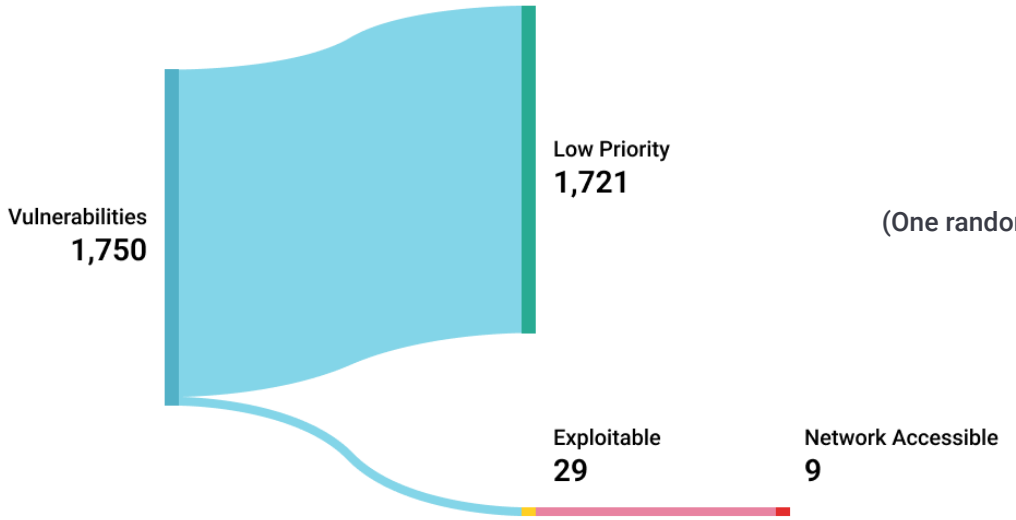
Now we know that in the 100 networking equipment devices there were 112,026 CVEs, and 2,022 total weaponized vulnerabilities. Next, we find that of the 2,022 weaponized vulnerabilities, 667 of those are network accessible (or approximately 7 per device).



Weaponized and Network Accessible Vulnerabilities

Weaponized and Network Accessible Vulnerabilities

When we randomly look at the data for a single networking equipment device, we found the following breakdown of vulnerabilities / CVEs, weaponized / exploited vulnerabilities, and network accessible weaponized vulnerabilities.



Weaponized and Network Accessible Vulnerabilities
(One randomly selected network device)

Unique Vulnerabilities by EPSS Score

We next look at the EPSS Score for each vulnerability. The EPSS allows companies to prioritize the most pressing vulnerabilities with threat actor information and a probabilistic understanding of threats. Be aware that EPSS Scores are temporal meaning they can change over time. So the data below represents a snapshot of the data from the day the research was generated.

There were 112,026 CVEs in the 100 networking equipment devices, but only 4,862 unique CVEs. Below we categorize these unique CVEs by the EPSS.

EPSS Score	Unique Vulnerability Count
above .90	38
between .80 and .90	4
between .60 and .80	9
between .20 and .60	20
below .20	4862

Total Vulnerabilities Categorized by Age

If we look at the 112,026 CVEs in the 100 networking equipment devices, we find that 37.2% of the CVEs are at least 5 years old or older. Below we categorize the CVEs by age.

Age	CVE Count
10+ years old	6843
5-10 years old	34817
2-5 years old	36889
1-2 years old	18601
6 months to 1 year old	7020
3-6 months old	4617
1-3 months old	3225
15 days to 1 month old	14

Software Vulnerability Reporting - Detailed Software Analysis versus Traditional Network Based Vulnerability Scanning

Lastly, we look at the vulnerability results when using the detailed Software Analysis detailed above in order to find known vulnerabilities per networking equipment device versus the more traditional Network Based Asset Scanning approach that relies on looking up Device Names and Versions on the NVD.

When manually compiling this data and comparing the results on a device by device basis we find that the detailed Software Analysis approach to vulnerability reporting uncovers 243.4 times more vulnerabilities than the more traditional approach of network based asset scanning finds from what is typically represented in the NVD.

Per Device CVEs Found	**Using Detail Software Analysis**	**Using Traditional Scanning (NVD)**
Total CVEs	1120.3	4.6
Weaponized CVEs	20.2	n/a
Weaponized and Network Accessible CVEs	6.7	n/a

Summary

Today's world is built on software – 3rd party software, open source software, in-house developed software, operating system software, applications, containers, and device firmware to name a few. In this research report we looked at a detailed analysis of the software on 100 different networking equipment devices focusing on five classes of devices, namely: routers, switches, firewalls, VPN gateways, and Wireless APs.

Software Bills of Materials Analysis: Using the detailed software analysis in the NetRise Platform, we find that the SBOM for the average network equipment device is quite complex and contains 1,267 software components.

Vulnerability Risks Analysis based on a Detailed Software Analysis Approach: Using the detailed software analysis in the NetRise Platform, we find that the average network equipment device has 1,120 known vulnerabilities, 20 weaponized vulnerabilities, and 7 weaponized and network accessible vulnerabilities.

Analysis Methodology and Approach: First, every piece of software, no matter how reputable the source, is quite complex and poses risks. Second, it's critical that those that build, buy, use, and maintain the software can inventory and understand the scope and scale of their software, and the associated risks. Finally, we believe a deep analysis of the software using a compiled and interpreted code analysis is the only way to get to this information.

Making this Software Supply Chain Research Actionable: In general, companies do not control the software on their networking devices and cannot patch the CVEs on these devices. And as we see, there are so many CVEs on average on each networking device (1,120) the average company could never patch even a fraction of these CVEs. And, using CVSS is not the best way to prioritize CVEs as we have seen since more High and Medium Severity CVEs are exploited than Critical Severity CVEs. We recommend a software supply chain analysis of the software and vulnerabilities and using weaponized and network accessible CVEs as a starting point in prioritizing the CVEs on networking equipment.

End Notes

1. 9th Annual State of the Software Supply Chain, Sonatype.
2. Three in Five Businesses Affected by Software Supply Chain Attacks in Last 12 Months, Gartner/Capterra, May 11, 2023.
3. The Riskiest Connected Devices in 2024, Forescout, June 10, 2024.
4. The State of Software Supply Chain Security Risks, Prepared by Ponemon Institute, Sponsored by Synopsis, May 2024

Glossary of Terms

CISA KEV - The Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog is a compilation of documented security vulnerabilities that have been successfully exploited, as well as vulnerabilities associated with ransomware campaigns.

CISO - Chief Information Security Officer.

CVE - The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures.

CVSS - The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

EPSS - The Exploit Prediction Scoring System (EPSS) is a data-driven effort estimating the likelihood (probability) that a software vulnerability will be exploited in the wild.

IoT - The Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. The Internet of things encompasses electronics, communication, and computer science engineering.

IT - Information Technology.

NVD - The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data.

SBOM - A “software bill of materials” (SBOM) has emerged as a key building block in software security and software supply chain risk management. An SBOM is a nested inventory, a list of ingredients that make up software components.

XIoT - The extended internet of things (XIoT) is an umbrella term that includes all internet of things (IoT) or physical devices connected to the internet. It encompasses networking equipment, IoT, operational technology (OT), internet of medical things (IoMT), industrial IoT (IIoT), and supervisory control and data acquisition (SCADA).