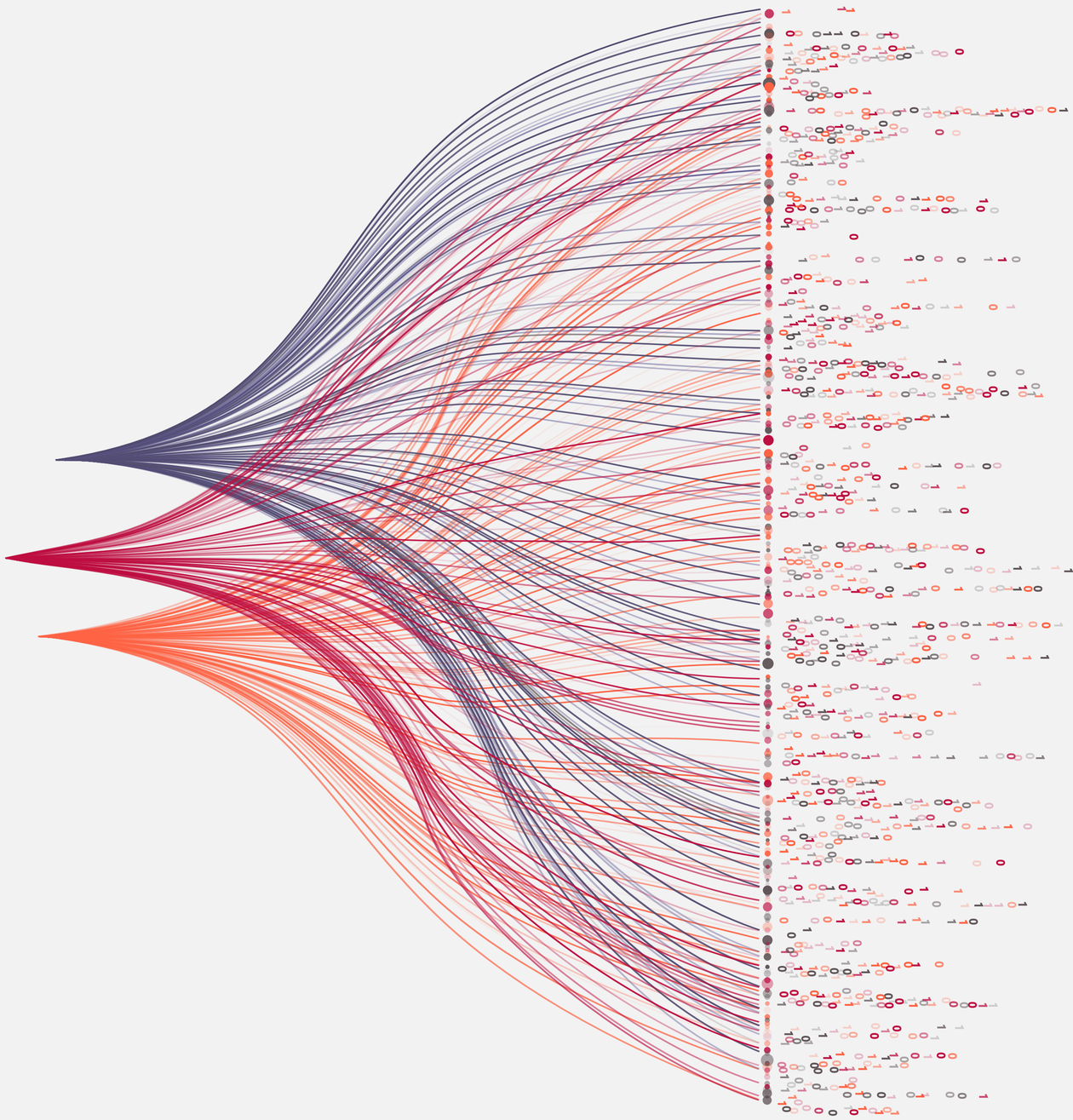
SPOTLIGHT REPORT 2023

RANSOMWARE

Through the Lens of Threat & Vulnerability Management



Securin | CSW Cyber SecurityWorks | ivanti | CYWARE™

Table of Contents
Introduction
Executive Summary
Report Methodology
Key Findings
Ransomware Metrics
MITRE Analysis
Scanner and Weakness Analysis
Latency Analysis
Special Snapshot: Cybersecurity in the US States
Predictive Insights
Noteworthy Trends and Interesting Facts
Future Predictions
Conclusion
About Us
Appendix

TABLE OF CONTENTS

Introduction

Thank you for your continued interest in our cybersecurity research program and ransomware reports! We are happy to inform you that Cyber Security Works (CSW) has rebranded itself as Securin INC. By rebranding, CSW combines its flagship services (Vulnerability Management and Penetration Testing) along with Securin's products (Attack Surface Management and Vulnerability Intelligence). Powered by actionable intelligence based on Artificial Intelligence (AI), machine learning (ML), automation, and the human expertise of our security teams, Securin's tech-enabled services will provide customers with a meticulous and comprehensive view of their attack surface.

As Securin, we will continue to publish our research in collaboration with our partners and help customers identify key threats and trends that could impact their business operations. As always, we have collaborated with our partner Ivanti to publish this ransomware report.

Since its first publication in 2019, many organizations and customers have used our ransomware reports as a guide to understanding the nature of these threats. In 2021, we saw a huge surge in ransomware vulnerabilities, prompting us to publish quarterly updates and trends. Unfortunately, there has never been a quarter where the number of ransomware vulnerabilities has not increased. In this report, we analyze the newly associated vulnerabilities from the past year and the last quarter and present to you overall trends, observations, and recommendations to counter such threats.

Executive Summary

Ransomware has become an escalating problem. We have been tracking this menace since 2020 and have watched the threat progress from becoming a pesky headache to a deployable weapon. From causing the death of patients in critical condition to disrupting the supply of the Colonial Pipeline for an entire week on the East Coast of the US, ransomware attacks are becoming more hazardous, daring, and audacious. In the past year, a 150-year-old college in Illinois had to close its operations, becoming the first educational institution to permanently shut down due to a ransomware attack. Unfortunately, it may not be the last.

Costa Rica had to declare a state of emergency because of an attack on its government agencies. The attack was so crippling that the country's tax collection was interrupted and citizens' personal information became exposed. In the past year, we have also seen ransomware being deployed as a choice of cyber weapon in the ongoing conflict between Russia and Ukraine and ransomware operators like Conti declaring allegiance to the former and attacking its adversaries.

In the last few years, we have seen how ransomware groups have matured and become more sophisticated in their operations. From a trend perspective, we are seeing a higher adoption of ransomware attacks among threat groups that use ransomware as a weapon against their targets. The deployment of ransomware as a precursor to an actual, physical war is another trend that began with the cyber warfare between Russia and Ukraine and one that will probably continue.

In this report, we have examined the existing gaps in MITRE repositories and how they inhibit security teams from understanding their true threat context. We also introduce Securin's Vulnerability Risk Score (VRS), an alternate vulnerability ranking system that can help organizations prioritize vulnerabilities based on their risk factors, threat associations, exploitability, and criticality. Securin VRS is currently being used in all our products and services to help our customers understand the true risk of a vulnerability and its ability to be weaponized and potentially exploited.

In the snapshot section, we include our investigation into the cyber hygiene of all US State domains and associated websites. Through this snapshot, we hope to aid CISA in its national effort to improve cyber resilience in all government infrastructure, help shrink attack surfaces, and remediate vulnerabilities before they are exploited.

Report Methodology

The information in this report is based on data gathered by Securin's security researchers and threat hunters and from the ransomware data maintained in Securin's Vulnerability Intelligence (VI) platform, along with Ivanti's research data.

Our ransomware data is meticulously collated from multiple data sources known for their accuracy and is continuously updated by Securin's research teams. Our security researchers and penetration testers use this data to improve our clients' security posture and keep them safe from evolving ransomware threats and risks. The report aims to highlight key findings related to ransomware, increase ransomware literacy, and share actionable insights with our community to eliminate vulnerabilities associated with ransomware in their environments.

Securin's research methodology focuses on definitive and predictive data to drive our security intelligence. The definitive analysis encapsulates specific vulnerability and threat data continuously cleansed, enhanced, and validated by our researchers. Our predictive analysis leverages data from Securin VI collected from open, social, deep, and dark web sources. It then leverages more than 60 Machine Learning (ML) models to predict if a vulnerability will be exploited in the wild. This approach of combined research provides comprehensive coverage and predictive intelligence to reduce ransomware risks significantly.

In this report, we have also introduced a new vulnerability scoring methodology called the Vulnerability Risk Score (VRS) used in Securin's platform products—Securin ASM and Securin VI. The VRS takes a two-pronged approach to compute a vulnerability's risk: definitive and predictive. It is based on a scale of 0–10 for those with definitive threat associations (such as public exploits, ransomware, and APT groups), and 1–38.4615 for predicting their likelihood of exploitation, considering more criteria and parameters to determine the risk posed by a CVE. For more information about the VRS, please check out our detailed blog.

In this report, we have defined parameters for two important criteria that are used to analyze and understand the risks posed by a vulnerability:

- **Old Vulnerabilities:** Securin VI classifies vulnerabilities discovered from 2010 to 2019 as old.

- **Trending Vulnerabilities:** In this report, we have combined two important trending pieces of information sourced from Ivanti Neurons for Risk-Based Vulnerability Management (RBVM) platform and Securin VI. The latter considers vulnerabilities and threats (exploits or malware) of interest that are searched on the surface web and trending at the top of search charts.

The Special Snapshot section of this report provides data on the ransomware susceptibility of the state entities in the US. This data was gathered by passively scanning domains belonging to state entities of all 50 states. In this section, we examine the attack surface—region-wise—to see what threats might slip through the cracks in their defense.

Key Findings

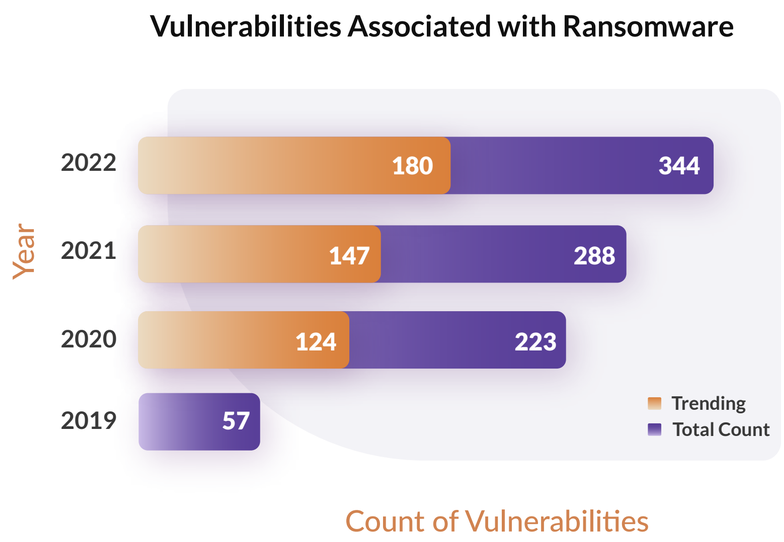
Vulnerabilities Associated with Ransomware Continue to Increase

19% increase in the count of vulnerabilities associated with ransomware

Overall, 56 vulnerabilities became newly associated with ransomware threats in 2022, taking the total count to 344. In the last quarter of 2022, 21 vulnerabilities were exploited by ransomware, such as BlackByte, Hive, LockBit, Cerber, AvosLocker, OldGremlin, Ransom Cartel, RAR1Ransom, and Bisamware.

Our researchers also found that hackers and malicious actors were actively searching[1] the internet and the deep and dark web for 180 vulnerabilities associated with ransomware as a point of interest.

Know More



[1] Trending data is collated from the Securin Vulnerability Intelligence (VI) and Ivanti RBVM Platforms as of Dec. 20, 2022. The trending data cumulatively looked at vulnerabilities and threats(exploits/malware) of interest on the surface web.

A Complete ATT&CK Kill Chain[2] Exists for 57 Vulnerabilities Associated with Ransomware

81 unique end-to-end products can be exploited by ransomware groups

We mapped each ransomware-associated vulnerability to its MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and identified 57 vulnerabilities that are extremely dangerous and can be exploited from initial access to exfiltration. These vulnerabilities are found primarily in vendors such as Microsoft, Oracle, F5, VMWare, Atlassian, Apache, SonicWall, and many others, spanning 81 unique products.

Know More

Popular Scanners Do Not Detect Vulnerabilities Associated with Ransomware

20 vulnerabilities associated with ransomware are not detected by Nessus, Nexpose, and Qualys

Popular scanners such as Nessus, Nexpose, and Qualys do not detect certain vulnerabilities associated with ransomware, giving organizations a false sense of security. We identified 20 vulnerabilities associated with ransomware for which plugins and detection signatures are yet to be added. Unfortunately, this includes all vulnerabilities associated with ransomware we identified in the past quarter with two new additions—CVE-2021-33558 (Boa) and CVE-2022-36537 (Zkoss).

Know More

[2] A MITRE ATT&CK kill chain is a model where each stage of a cyberattack can be defined, described, and tracked, visualizing each move made by the attacker. Using this framework, security teams can stop an attack and design stronger security processes to protect their assets.

More APT Groups Use Ransomware to Attack Their Targets

4 new APT groups are deploying ransomware in their arsenal

Advanced Persistent Threat (APT) groups are adding ransomware as part of their threat arsenal to target their victims. In 2020, 33 APT groups were observed deploying ransomware to mount their attacks, and this count increased to 50 in 2022.

In the last quarter, four new APT groups emerged— DEV-023, DEV-0504, DEV-0832, and DEV-0950—and deployed ransomware to infiltrate and mount crippling attacks. We observed DEV-0832 using Vice Society, Zeppelin, and BlackCat ransomware to target its victims belonging to the education, government, and retail sectors, respectively. DEV-023 and DEV-0504 use the BlackCat ransomware as a weapon of choice to attack and infiltrate their targets. DEV-0950 uses two ransomware groups—CLOP and CryptoMix ransomware families—to target their victims.

Know More

Vulnerabilities Associated with Ransomware Excluded from CISA Known Exploited Vulnerabilities

131 vulnerabilities associated with ransomware are yet to be added to the CISA KEV catalog

CISA launched the Known Exploited Vulnerabilities (KEVs) catalog to remediate oft-exploited vulnerabilities that exist in the Federal Civilian Executive Branch (FCEB) and the public sector entities. This catalog has 866[3] vulnerabilities that the FCEB is mandated to remediate by CISA's directive. While all the KEVs are weaponized and actively exploited by adversaries, our experts observed that 213 vulnerabilities associated with ransomware had been added to the catalog, and 131 have been excluded.

Know More

[3] As of Dec. 15, 2022

Vulnerabilities Associated with Ransomware Present in Multiple Products

118 vulnerabilities associated with ransomware impact multiple products

In 2022, six vulnerabilities that exist in multiple products have become associated with ransomware, such as Satan, AvosLocker, BigBossHorse, and RAR1Ransom. Reusing open source code in software products results in the replication of the same vulnerability in multiple products. For example, CVE-2021-45046—an Apache Log4j vulnerability—is present in 93 products from 16 vendors and is exploited by the AvosLocker ransomware. CVE-2021-45105—another Apache Log4J vulnerability—is present in 128 products from 11 vendors and is also exploited by the AvosLocker ransomware.

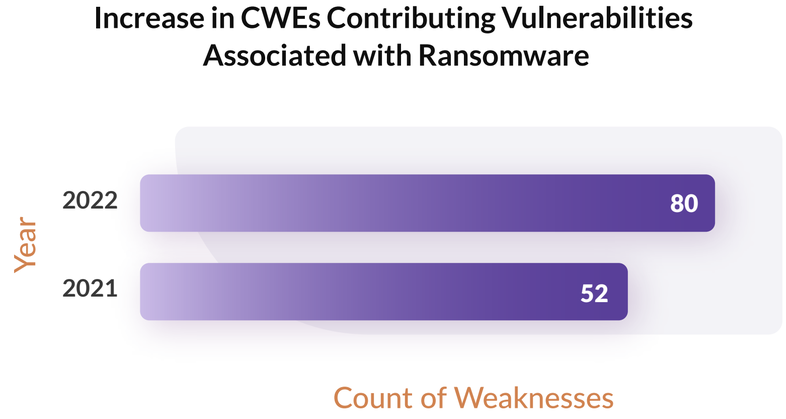
Know More

Increase in New Weakness[4] Categories

80 CWEs contribute vulnerabilities exploited by ransomware

Overall, 80 CWEs[5] are contributing vulnerabilities that are exploited by ransomware operators. We have observed a consistent increase in this trend year after year, highlighting the need for software vendors and application developers to evaluate their software code before it is released. This also spotlights the need to shift left and test the foundational code of software products even while it is in production.

Know More



[4] MITRE describes "weaknesses" as flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture that—if left unaddressed—could result in systems, networks, or hardware being vulnerable to attacks.

[5] Common Weakness Enumeration

Ransomware Operators Leverage Old Vulnerabilities[6]

76% of the ransomware-associated vulnerabilities are old vulnerabilities discovered before 2020

Old is still gold for ransomware operators. Overall, 76% of vulnerabilities exploited by ransomware are old—discovered between 2010 and 2019. In 2022, 56 vulnerabilities became tied to ransomware, out of which 20 were old vulnerabilities discovered between 2015 and 2019. These vulnerabilities are being exploited by notorious ransomware gangs, such as Conti, BlackCat, Hive, and BlackByte.

Know More

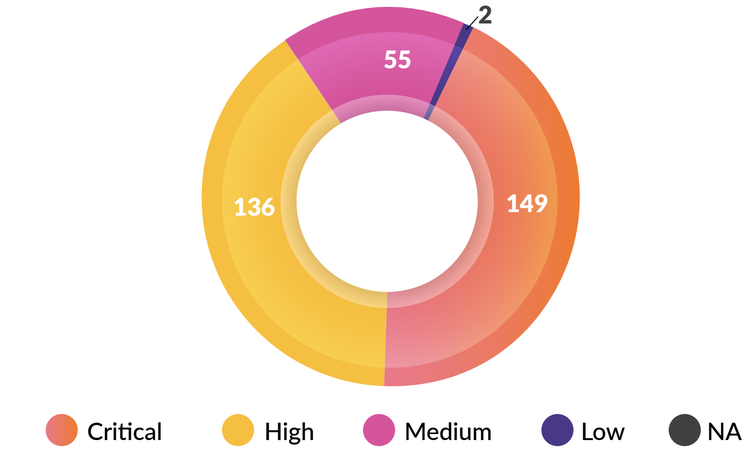
High-Risk Vulnerabilities Associated with Ransomware Fly Beneath the Radar

16% of the vulnerabilities associated with ransomware have low and medium CVSS scores

We found 57 ransomware-associated vulnerabilities (16%) with low and medium CVSS scores. This provides a false sense of security for those organizations who follow CVSS scores to prioritize their vulnerabilities. These vulnerabilities are associated with infamous ransomware families such as Conti, LockBit, AvosLocker, and BlackCat and exist in Red Hat (Enterprise Linux), Microsoft (Windows Server 2008 and 2012 and Windows 7), Novell (openSUSE), CentOS, and Amazon (Linux).

Know More

Severity Scores of Vulnerabilities Associated with Ransomware



[6] Securin's experts consider vulnerabilities discovered between 2010 and 2019 as old. The same rule also applies to vulnerabilities discovered before 2010.

Definitive Insights

Securin | CSW Cyber SecurityWorks | ivanti | CYWARE™

Definitive Insights

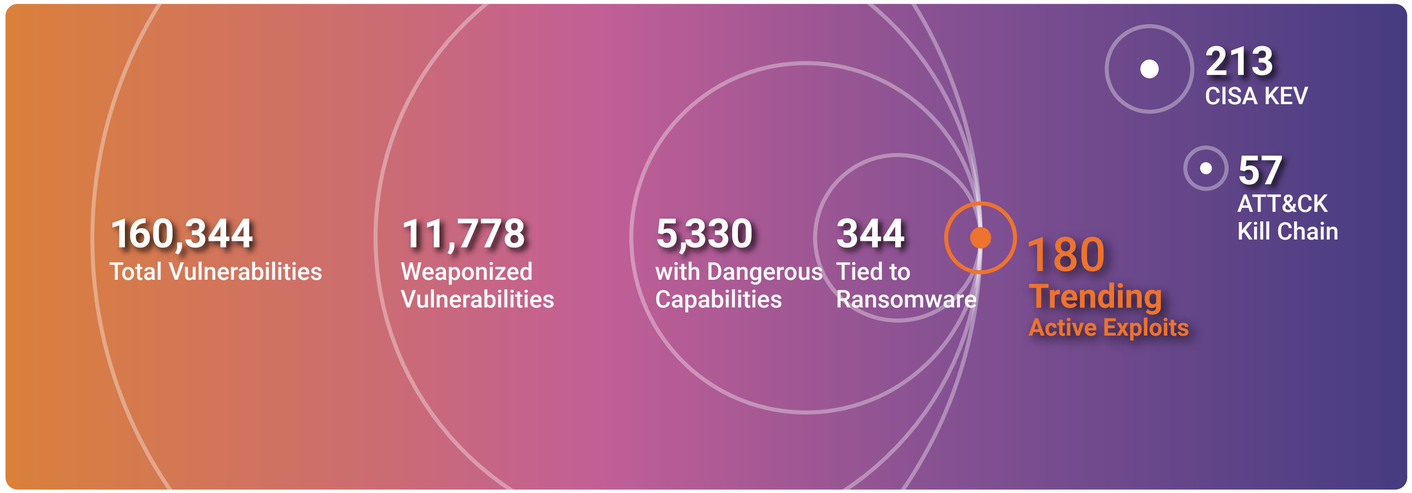
Ransomware Metrics

Ransomware has been around for decades. What was earlier considered an inconvenience has now become an escalating threat that can disrupt business operations, sabotage critical infrastructure, force businesses to close down, ruin reputations, and cause death.

We have been tracking this pervasive menace since 2019 and have seen the count of vulnerabilities increase by 503% since then. In 2022, a 19% increase in vulnerabilities was observed as 56 vulnerabilities became newly associated with notorious ransomware, such as Conti, QLocker, BlackCat, FiveHands, AvosLocker, Hive, and nine others.

Key Vulnerability Metrics and Risk Factors

To understand the ransomware threat better, we use a risk-based approach to segment vulnerabilities based on their threat context.



Weaponized Vulnerabilities

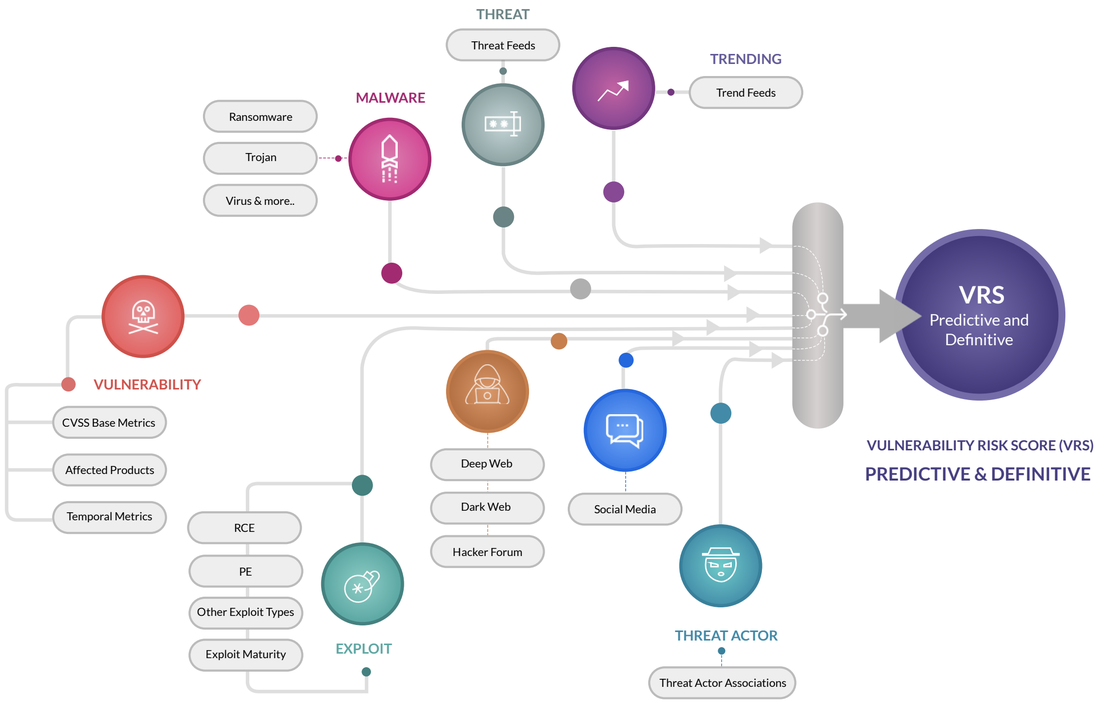
Today, there are 160,344 vulnerabilities[7] listed in the National Vulnerability Database (NVD), of which 3.3% (5,330) belong to the most dangerous exploit types—Remote Code Execution (RCE) and Privilege Escalation (PE). Out of the 5,330 weaponized vulnerabilities, 344 are associated with 217 ransomware families and 50 Advanced Persistent Threat (APT) groups, making them extremely dangerous. We also observed that exploits for 275 vulnerabilities associated with ransomware are available right now in the public domain, meaning you cannot afford to ignore them.

High Risk of Low-Score Vulnerabilities

From an overall perspective and looking at the CVSS V2 severity ratings, 66% of vulnerabilities associated with ransomware have been rated high, whereas CVSS V3 rates 26% as critical and 35% as high. If organizations followed these critical and high severity ratings to prioritize their patching cadence, they would still be exposed to vulnerabilities associated with ransomware that have been rated low, medium, or worse—those that have no ratings.

To fill this gap, Securin Vulnerability Intelligence (VI) introduces the Vulnerability Risk Score (VRS) to help organizations understand the threat context associated with vulnerabilities and prioritize their patching accordingly.

What Goes into Our VRS

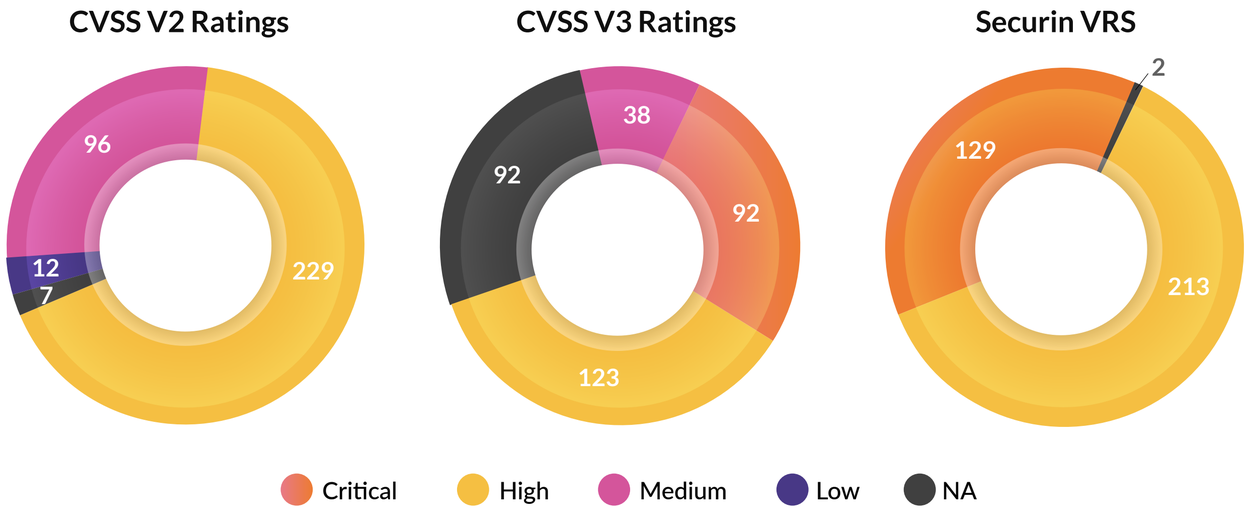


[7] As of Dec. 15, 2022

The VRS considers many factors, such as the maturity of the exploits, the exploit type, threat associations (ransomware and APT groups), trending analysis, and the potential impact of exploitation, to assign scores to each vulnerability. The VRS also measures vulnerabilities based on a scale of 0–10 for those with definitive threat associations (such as public exploits, ransomware, and APT groups), and 1–38.4615 for predicting their likelihood of exploitation, considering more criteria and parameters to determine the risk posed by a CVE.

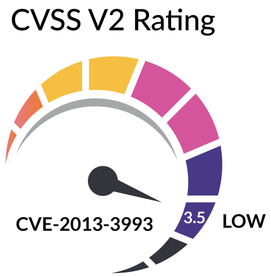
When we analyzed the overall severity scores of vulnerabilities associated with ransomware by applying the VRS, we found 61% rated as critical and 37% as high. This affirms our approach that any vulnerability that becomes tied to ransomware should be considered high risk and must be prioritized for patching. The VRS eliminates this ambiguity and gaps in information that exist in the CVSS V2 and V3 scoring methodology and provides a definite score by assessing the risk continuously based on past and current events.

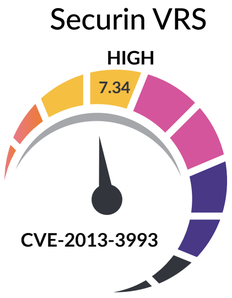
Severity Scores of Ransomware-Associated Vulnerabilities

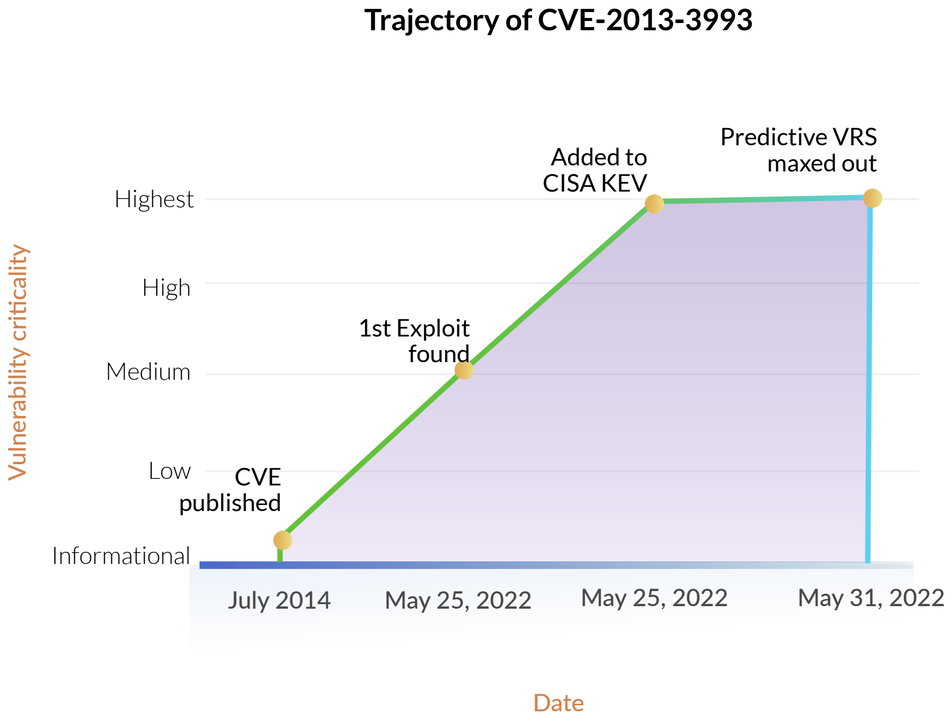


Now, let us turn our attention toward medium and low CVSS ratings. The CVSS V2 methodology rates 31% of vulnerabilities as low or medium, while CVSS V3 considers 10% of vulnerabilities as medium severity. There are 26% of vulnerabilities that do not have a CVSS V3 rating; so organizations that assiduously follow only CVSS ratings have no clue about their threat context. Even so, most organizations prioritize critical and high vulnerabilities for patching, but it is the medium- and low-rated vulnerabilities exploited by ransomware that fly under the radar.

For example, let us examine CVE-2013-3993, a vulnerability that exists in IBM Infosphere BigInsights. IBM Infosphere BigInsights is a platform designed to help organizations analyze business insights from large volumes of diverse data. CVSS V2 rates this vulnerability as 3.5 (low). Since this CVE was discovered before 2015, CVSS V3scores are unavailable. This vulnerability is associated with two ransomware gangs—Petya and Locky. An exploit for this CVE was published on May 25, 2022. On the same day, CISA included this vulnerability in the KEV catalog. On May 31, 2022, this vulnerability got the maximum predictive score (38.46) on the Securin VI platform, and Securin VRS rates this vulnerability as high with a rating of 7.34.

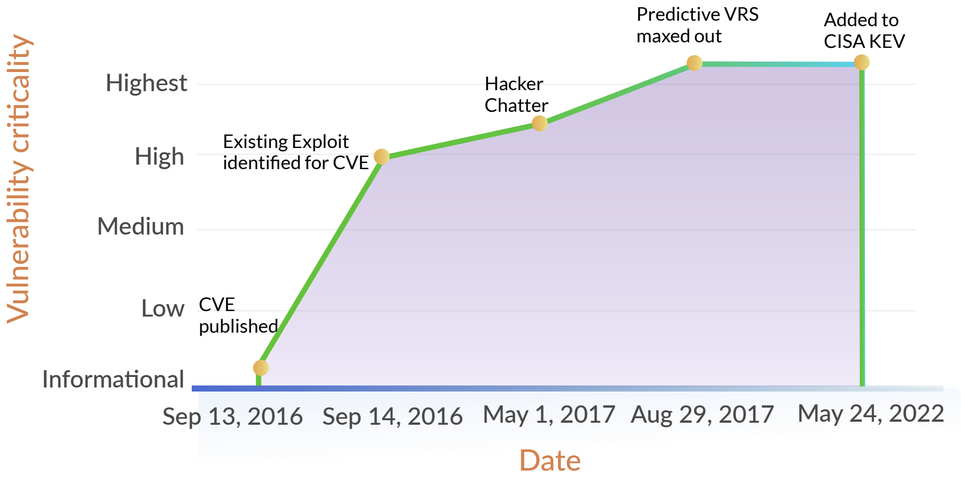






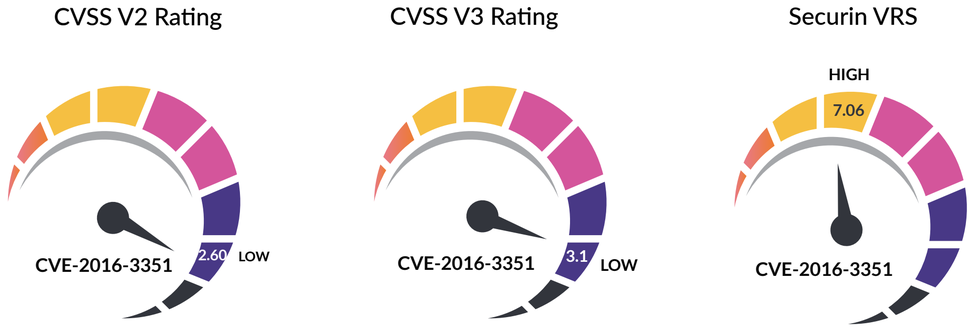
CVE-2016-3351 is yet another interesting example. This Microsoft vulnerability (Internet Explorer, Edge, Windows Server 2008 and 2012, and Windows 8 and 10) gets a low score both in CVSS V2 (2.60) and V3 (3.1) and is exploited by nine ransomware gangs—Cryptesla, Better_call_saul, CrypBoss, CrypWall, Waltrix, JuicyLemon, Kovter, Reveton, and TorrentLocker. On May 24, 2022, this vulnerability was added to CISA KEVs, and we found it trending on the internet as of December 12, 2022. The Securin VRS rates this vulnerability high, with a VRS of 7.06.

Trajectory of CVE-2016-3351



NOTE: Exploit for CVE-2016-3351 was available even before the CVE could be officially published.

Severity Score Comparison for CVE-2016-3351



Low-score vulnerabilities can be used in vulnerability chaining, a well-established technique used by threat actors during the reconnaissance process, to identify direct or peripheral vulnerabilities and weaknesses—both in hardware and software—and exploit them at the same time to compromise the target host. Let us look at the vulnerability chaining of Microsoft Exchange ProxyShell and Windows PetitPotam vulnerabilities that were chained together in August 2021 by the LockFile ransomware. The ransomware gang actively abused the faulty patch to the PetitPotam vulnerability post-exploitation to gain access to domain controllers and spread across the network.

CVE-2021-36942 is a medium-severity vulnerability rated 5 and 5.36 in CVSS V2 and V3, respectively. When chained along with critical vulnerabilities such as CVE-2021-34523 and CVE-2021-34473 and a high-severity vulnerability (CVSS V3) CVE-2021-31207, it becomes a moving part of a dangerous weapon.

The FiveHands ransomware makes yet another classic example of vulnerability chaining in recent times. This gang went after four vulnerabilities associated with ransomware, including a medium-severity CVE, CVE-2021-20023, in SonicWall to create a complete kill chain.
The infamous Pegasus spyware makes a great example here when the attackers chained Trident iOS vulnerabilities—CVE-2016-4655, CVE-2016-4656, and CVE-2016-4657—to jailbreak iPhones during an attack. In this instance, CVE-2016-4655 was a medium-severity vulnerability with a CVSS V3 rating of 5.50.

With the increasing instances of vulnerability chaining, our researchers worked with MITRE ATT&CK mapping to check how it can help identify vulnerability chaining. Let us see how we analyzed and identified a vulnerability chaining possibility in Q4 2022 before ransomware actors could exploit the same, thus helping our customers prioritize and patch the vulnerabilities on time.

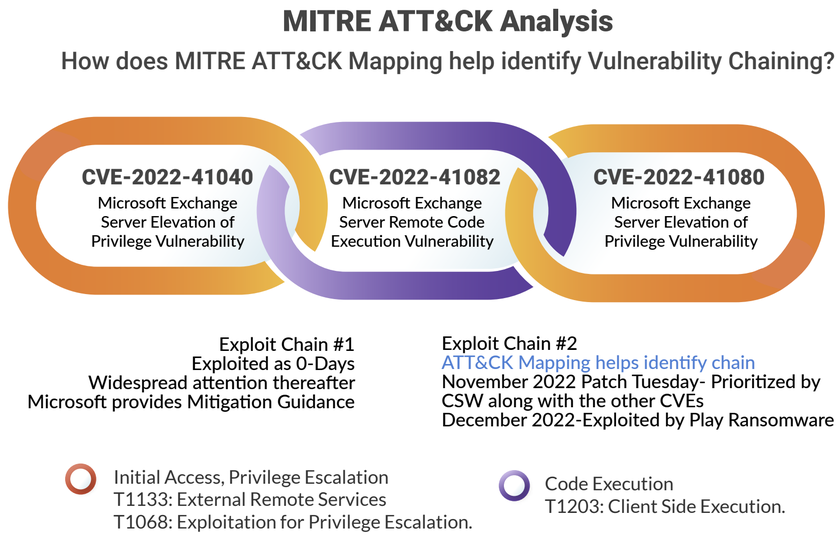
In November 2022, the ProxyNotShell vulnerabilities were exploited as zero-day vulnerabilities, and two CVEs—CVE-2022-41082 and CVE-2022-41040—were called out as heavily trending. Threat actors used the former to escalate privileges, while the latter helped execute custom code remotely. The Microsoft vulnerabilities were patched and provided with mitigation guidance as well.

However, using MITRE analysis, our analysts observed another vulnerability, CVE-2022-41080, with capabilities similar to CVE-2022-41082, which could be linked to CVE-2022-41040 to execute an attack.

In the following month, the Play ransomware used this lesser-known second vulnerability chain to attack Rackspace Technology and executed a ransomware attack, affecting its environment, disrupting services, and extracting sensitive customer data.

Know more about our detailed analysis of MITRE mapping of vulnerabilities associated with ransomware.

Adversaries are always on the lookout to weaponize vulnerabilities that are not on the radar of the security teams.



Here is a classic example:

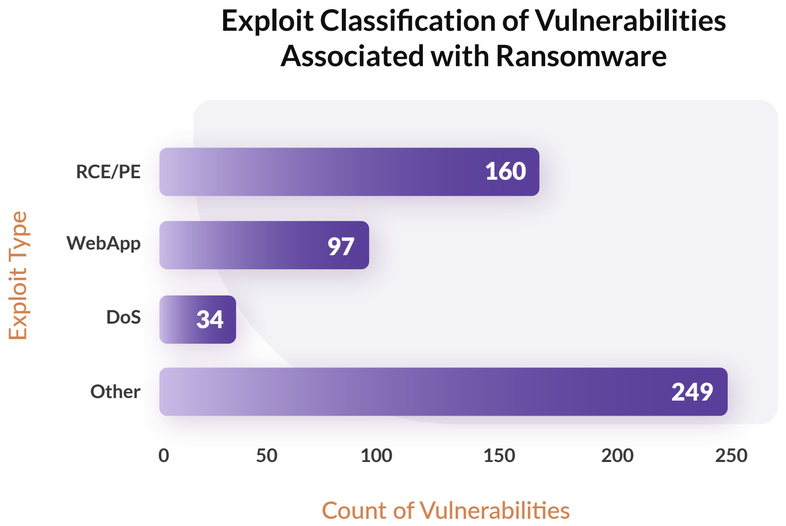
Two vulnerabilities (CVE-2015-2551 and CVE-2019-9081) have been tagged as 'Rejected' by the National Vulnerability Database, but they have ransomware associations. CVE-2015-2551 is associated with 17 ransomware gangs, notably Cerber, CrypWall, Locky, Reveton, Better_call_saul, and 12 others. Interestingly, there is no vendor or product information available in the NVD for this vulnerability.

CVE-2019-9081 is yet another 'Reject' vulnerability that is associated with two ransomware gangs, Mailto and Satan. There is no information about severity ratings or products for this vulnerability though we have been able to verify that this CVE was assigned to a Laravel framework product and was later withdrawn because it is not a security issue anymore (as per the message posted in the NVD). As of December 05, 2022, we found this CVE trending in the deep and dark web, which indicates hackers' interest in it. It is these kinds of drawbacks that adversaries love to exploit, especially when repositories—like the NVD—have no information to offer.

From a threat perspective, once a vulnerability becomes associated with ransomware, it should be considered high risk. That is why we reiterate that organizations solely dependent on CVSS scores will be at risk from vulnerabilities such as these unless they augment their prioritization with additional threat intelligence.

Exploit Types and Weaponization

Over the past year, we have observed the constant growth of weaponized vulnerabilities. While the count grew by 473 in 2021, the increase was trifold, with an uptick of 1,410 vulnerabilities in 2022. Although the growth of those associated with ransomware reduced from 65 (in 2021) to 56 (in 2022), the increase is still alarming. The continued growth of vulnerabilities associated with ransomware is an indication that ransomware groups are constantly on the lookout for vulnerabilities to add to their arsenal, thus compromising exposed networks.



We also analyzed the growth of these ransomware-associated vulnerabilities over the past year and identified a definite increase in vulnerabilities with publicly available exploits. Clearly, ransomware actors do not miss the opportunity to add such powerful vulnerabilities to their arsenal. Of these, Remote Code Execution (RCE) and Privilege Escalation (PE) are the most dangerous exploits that hackers are keen to weaponize.

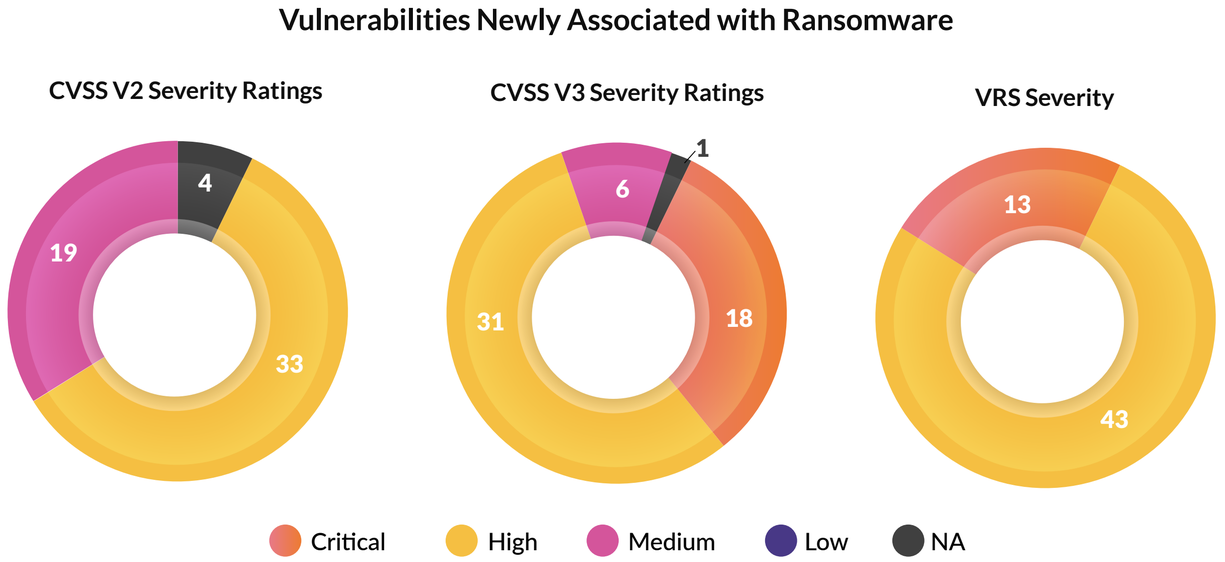
	Dec. 2021	Dec. 2022	Percentage Growth
Ransomware CVEs with exploits	164	275	67.68
RCE	109	131	20.18
PE	23	91	295.65
DoS	13	34	161.54
WebApp	40	97	142.5

Newly Associated Vulnerabilities

Next, we analyzed the vulnerabilities that have become associated with ransomware in the past year. Totally, 56 vulnerabilities became tied to ransomware in 2022, taking the total count of ransomware CVEs to 344. Out of 56, 20 vulnerabilities—accounting for 35%—are old vulnerabilities discovered between 2015 and 2019. This proves that adversaries are counting on your lack of cyber hygiene to launch their attacks.

Next, we examined the severity scores of these newly associated vulnerabilities using CVSS V2, V3, and the Securin VRS to understand the threat context of these CVEs.

CVSS V2 and V3 scores were not available for four vulnerabilities and one vulnerability, respectively. This gap in information is advantageous to adversaries as they go ahead and weaponize such CVEs. For security teams, this is a huge drawback as they neither have the time or resources to research these CVEs nor determine their threat context. Securin VRS easily solves this challenge, as you can see that 43 (out of 56) vulnerabilities are given high scoring while 13 of them are considered critical.



Next, we examined the exploit type and found that 23 (out of 56) were RCE/PE with exploits that were available in the public domain. Interestingly, CISA has already added 46[8] of these vulnerabilities to the KEV catalog though we recommend that they add the rest as well.

[8] As of Dec. 15, 2022

The following are the top five vendors where these vulnerabilities newly associated with ransomware exist:

Top Five Vendors with Vulnerabilities Newly Associated with Ransomware

Vendor Name	Count of Vulnerability Associated with Ransomware
Microsoft	24
SonicWall	5
VMWare	3
Red Hat	3
QNAP	3

Top Five Most Affected Products

Product Name	Count of Vulnerability Associated with Ransomware
Microsoft Windows [9]	24
Microsoft Windows 10	22
Microsoft Windows Server 2019	20
Microsoft Windows Server 2016	20
Microsoft Windows Server 2012	15

Trending Vulnerabilities

When we compare trending vulnerabilities year after year, we find the number increasing as bad actors are constantly on the lookout for entry points that would allow them to take the entire house down. In 2022, 180 vulnerabilities associated with ransomware were found trending in the dark and deep web as a point of interest for malicious actors. Interestingly, 63% (out of 180) of them are old vulnerabilities ranging from 2008 to 2019. The oldest among them is CVE-2008-2992—an RCE vulnerability in Adobe—and is associated with the Crilock ransomware. The fact that bad actors are still interested in old vulnerabilities puts the spotlight firmly on the lack of cyber hygiene in our digital landscape. Never forget that these old and weaponized vulnerabilities are a potent mix that malicious actors are determined to exploit to mount crippling attacks.

[9] Includes multiple versions affected by the vulnerabilities

Vendors Under Attack

From the product and vendor standpoints, there are 115 unique vendors and 1,112 products that have vulnerabilities exploited by ransomware. The following are the top five vendors with the maximum number of vulnerabilities associated with ransomware. Microsoft products stand at the top of the list, with 44% of vulnerabilities associated with ransomware belonging to this vendor, followed by Red Hat products, which make up 25% of vulnerabilities.

Top Five Vendors with Maximum Vulnerabilities Associated with Ransomware

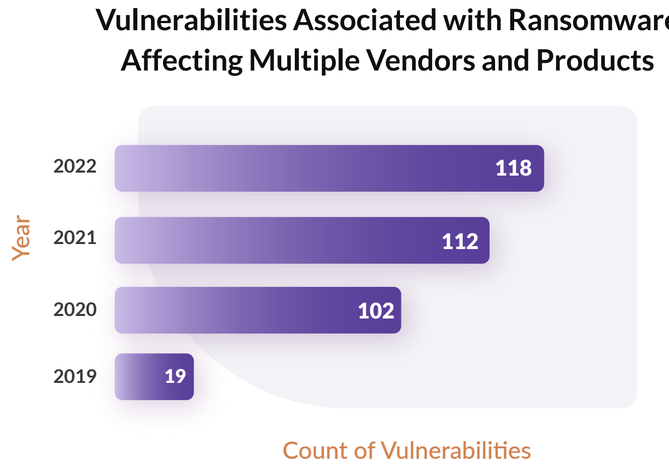
Vendor	Vulnerability Count
Microsoft	152
Red Hat	89
Novell	82
Gentoo	73
Oracle	61

Top Products with the Maximum Vulnerabilities Associated with Ransomware

Product	Vulnerability Count
Microsoft Windows[10]	133
Red Hat Enterprise Linux	85
Gentoo Linux	84
Novell openSUSE	78
Microsoft Windows Server 2002	75

[10] Includes multiple versions affected by the vulnerabilities

Vulnerabilities Associated with Ransomware in Multiple Products



Next, we examined vulnerabilities associated with ransomware that exist in multiple vendors and products. Unfortunately, this is a growing trend year after year.
Overall, 118 vulnerabilities exist in multiple products. This happens due to the reuse of code that replicates the same vulnerability in all products. The following are among the top five vulnerabilities that exist in the highest number of products:

CVE-2018-3639: A vulnerability rated as low in CVSS V2 (2.10), medium in CVSS V3 (5.5), and high in the Securin VRS (7.77) may allow unauthorized disclosure of information to an attacker. This vulnerability exists in 26 vendors and a whopping 345 products. Notable among them are vendors such as Red Hat, Oracle, Amazon, Microsoft, Apple, VMWare, and many others. This vulnerability exists in products such as Windows Server, Enterprise Linux Server, and many others and is associated with the Stop ransomware. We also found this vulnerability trending on the internet as of December 10, 2022.

CVE-2021-44228: A high-risk vulnerability rated critical in CVSS V3 (10) exists in Apache Log4j. This vulnerability exists in 176 products from 21 vendors. Notable among them are vendors such as Oracle, Red Hat, Apache, Novell, Amazon, Cisco, SonicWall, and others. This RCE vulnerability is exploited by six ransomware gangs: AvosLocker, Conti, Khonsari, Night Sky, Cheerscrypt, and TellYouThePass. This vulnerability, too, is a point of interest for hackers and was found trending as of December 10, 2022, which is probably why CISA has included it as part of the CISA KEV catalog.

CVE-2021-45046: This high-risk vulnerability is rated critical in CVSS V3 (9), and it exists in 16 vendors and 93 products. Notable among the vendors that are vulnerable to this CVE are Intel, Apache, NetApp, Red Hat, and many others. This vulnerability was newly associated with the AvosLocker ransomware in 2022 and had been trending since December 12, 2022. CISA has not prioritized this vulnerability as a KEV yet, but it is highly recommended that CISA adds it to the catalog.

CVE-2018-5391: This is an old vulnerability rated high in CVSS V3 (7.5), and it exists in 19 vendors and 40 products. This vulnerability exists in vendors such as Amazon, Debian, Oracle, Red Hat, Huawei, VMWare, Palo Alto Networks, Linux, and many others. The Stop ransomware is exploiting this vulnerability, and it was found to be trending as of December 13, 2022.

CVE-2020-1472: This is a high-risk vulnerability rated critical in CVSS V3 (10), and it exists in 18 vendors and 27 products. A few of the prominent vendors are Microsoft, Oracle, Red Hat, Amazon, openSUSE, and others. This vulnerability affects products such as Windows Server, Edge, Linux, Ubuntu Linux Directory Server, and many others. Classified as Privilege Escalation (PE), this vulnerability is exploited by nine ransomware gangs—Babuk, CryptoMix, Conti, DarkSide, Epsilon Red, Ryuk, Thanos, Hive, and Black Basta—and was found to be trending as of December 10, 2022.

Vulnerabilities associated with ransomware in multiple products pose a challenge for security teams and provide attackers with a multitude of opportunities to attack their victims. In 2022, six vulnerabilities—CVE-2017-8046, CVE-2020-0601, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105, and CVE-2022-22954—in multiple products came under the ransomware radar. These vulnerabilities are now being exploited by ransomware gangs such as Satan, BigBossHorse, AvosLocker, and RAR1Ransom.

Ransomware Gangs

When we analyzed the ransomware associations from the perspective of the threat context, we found 176 unique ransomware gangs exploiting 344 vulnerabilities. The Cerber ransomware stands at the top of the list with a whopping 72 vulnerabilities within its arsenal. CrypWall stands second with 66 vulnerabilities in its kitty, followed by the Locky ransomware with 64 vulnerabilities.

APT Groups That Use Ransomware Threats

Advanced Persistent Threat (APT) groups are not your run-of-the-mill hackers who infiltrate your network to steal data or hold it for ransom. Most have shadowy connections to hostile nation-states or—in some cases—are part of their military, actively aiding them in espionage, spying, and—in recent years—disrupting the critical infrastructure of countries that they deem as enemies.

One of the most dangerous trends we observed this year was the deployment of malware and ransomware as a precursor to an actual physical war.

Early 2022 saw the escalation of the war between Russia and Ukraine and the latter being attacked by APT groups—Gamaredon (Primitive Bear), Nobelium (APT29), Wizard Spider (Grim Spider), and Ghostwriter (UNC1151)—that targeted the critical infrastructure of Ukraine. We also saw Conti ransomware operators openly declaring their allegiance to Russia and attacking the US and other countries that supported Ukraine in this conflict. We believe this trend will continue to grow. The growth in the number of APT groups indicates the same.

As of December 2022, 50 APT groups are using ransomware as a weapon of choice to target their victims. Among the APT groups, Russia still leads the pack with 11 confirmed threat groups that claim origin and affiliations to the country. Among the most notorious APT groups from this region are APT28/APT29, which carried out the infamous SolarWinds attack to infiltrate and snoop. This threat group was observed deploying ransomware such as Golang, Petya, and Maze on its victims.

China follows as the second highest origin country for threat groups, with eight APT groups in its kitty. APT1, a shadowy Chinese-based threat group, stands at the top of the list. It goes by various aliases—GIF89a, Comment Crew, Comment Panda, Group 3, ShadyRAT, PLA Unit 61398, G0006, Byzantine Candor, TG-8223, Brown Fox, and many others—and loves to deploy the Maze ransomware as the weapon of choice.

North Korea has four APT groups affiliated with it and is the third country on this list. Among the APT groups that emerged in 2022, two groups (Andariel and DEV-0530) claim origins back to this country, and the ransomware of their choice is Maui and H0lyGh0st.

In 2022, ten new APT groups emerged and used ransomware as their arsenal:

Name of the APT Group	Origin Country	Name of the Ransomware
Andariel	North Korea	Maui
APT35	Iran	Memento
DEV-0401	China	Atom Silo, LockFile, Night Sky, Cheerscrypt
DEV-0530	North Korea	H0lyGh0st
Exotic Lily	Unknown	Conti
Tropical Scorpius	Unknown	Cuba
DEV-023	Unknown	BlackCat
DEV-0504	Unknown	BlackCat
DEV-0832	Unknown	Vice Society, Zeppelin, BlackCat
DEV-0950	Unknown	CLOP

We also analyzed this data from the perspective of ransomware to find out which ransomware is the most favored by threat groups. Here are our - top six

Old Vulnerabilities with Ransomware Associations

Of all vulnerabilities associated with ransomware, 76% of them are old, discovered between 2010 and 2019. Ransomware gangs are persistently going after old vulnerabilities and have been weaponizing them systematically. Out of the 264 old vulnerabilities, 208 of them have exploits that are publicly available. Of these, 131 have RCE/PE exploits, which make them extremely dangerous. What is more worrying is the fact that 119 of them are actively trending in the deep and dark web as a point of interest for hackers.

Interestingly, CISA has added 153 old vulnerabilities associated with ransomware in the KEV catalog as they are oft-exploited by threat actors and used as ransomware. This still excludes 111[11] old vulnerabilities with ransomware associations from the KEV list, a risk not addressed yet.

Next, we examined the vendor and products where the maximum number of these old vulnerabilities exist:

Name of the Ransomware	Count of APT Groups Using the Ransomware
Maze	7
DarkSide	5
Gimemo	4
WannaCry	4
BlackCat	3
CLOP	3

Vendors	Old Vulnerabilities Associated with Ransomware
Microsoft	118
Red Hat	82
Novell	75
Gentoo	70
Oracle	56

[11] As of Dec. 15, 2022

We next examined the most affected products where the maximum number of old vulnerabilities exist and many old suspects made an appearance.

Vendor	Most Affected Product	Count of Vulnerabilities Associated with Ransomware
Microsoft	Windows [12]	110
Red Hat	Enterprise Linux	78
Novell	openSUSE	71
Gentoo	Linux	70
Oracle	Linux	45

In 2022, 20 old vulnerabilities became newly associated with notorious ransomware gangs, such as Conti, BlackCat, Hive, and BlackByte. These vulnerabilities notably exist in the following vendors and products: Microsoft (Windows 10), Gigabyte (Xtreme Gaming Engine), MSI (Afterburner), and Boa (Boa).

Top Vendors with the Maximum Number of Old Vulnerabilities Newly Associated in 2022

Vendor	Most Affected Product	Count of Old Vulnerabilities
Microsoft	Windows 10	15
Gigabyte	Xtreme Gaming Engine	3
MSI	Afterburner	1
Boa	Boa	1

Top Products with the Maximum Number of Old Vulnerabilities Newly Associated in 2022

Product	Vendor	Count of Old Vulnerabilities
Windows 10	Microsoft	15
Windows [13]	Microsoft	15
Windows Server 2019	Microsoft	11
Windows Server 2016	Microsoft	11
Edge	Microsoft	11

[12] and [3] Includes multiple versions affected by the vulnerabilities

Interestingly, 18 vulnerabilities out of 20 that are not detected by the scanners are old CVEs discovered from 2010 to 2019. These findings bring the focus sharply back to cyber hygiene and the need for greater visibility of the attack surface and the assets used within it.

Legacy systems, unmanaged and unpatched components, and unknown shadow IT assets are favorite entry points for attackers. The continuous weaponization of old vulnerabilities reveals that adversaries love anything that would provide them an easy entry. Compound this with the fact that they exist in assets that you know nothing about, and your scanners do not detect them: it is a recipe for a perfect storm.

Vulnerabilities with Ransomware Associations in the CISA KEV Catalog

In November 2021, the Cybersecurity and Infrastructure Security Agency (CISA) issued a binding operational directive and published a catalog called Known Exploited Vulnerabilities (KEV) to aid the Federal Civilian Executive Branch (FCEB) and the public sector in reducing the risk of cyberattacks. This is a valuable initiative that can help the FCEB, public sector entities, and other organizations to keep pace with evolving and emerging threats. Since its publication, we have used this catalog as an essential vulnerability prioritization layer in our Vulnerability Management program.

The KEV catalog began modestly with 287 vulnerabilities and is now a repository of 866 CVEs[14] with strict deadlines to patch. When we analyzed the KEV catalog from a threat perspective, we found that 213 ransomware-associated vulnerabilities have been included in this living list, which is 61% of the total vulnerabilities associated with ransomware. Interestingly, we also observed that three vulnerabilities associated with ransomware (CVE-2019-1130, CVE-2019-1385, and CVE-2020-0638) that our experts recommended for inclusion on May 18, 2022, had become a part of the CISA KEV on May 23, 2022, which reaffirms our research.

See which top 10 ransomware-associated vulnerabilities should be included in the CISA KEV. VIEW LIST

For more information about the CISA KEV and the threat context, check out our Decoding CISA KEV reports, where we have analyzed the catalog based on the threat context and latency and have provided recommendations to include high-risk vulnerabilities that should be a part of this living list.

[14] As of Dec. 20, 2022.

MITRE Analysis

Our experts have been analyzing vulnerabilities associated with ransomware by mapping each CVE to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)[15] framework that provides security teams with deeper insights into adversarial behavior and attack patterns.

ATT&CK Kill Chain Vulnerabilities

By mapping all 344 vulnerabilities associated with ransomware, we identified the 57 most dangerous vulnerabilities (see our Q2-Q3 Ransomware Report) that could be exploited from initial access to exfiltration.

What is the MITRE ATT&CK Kill Chain?

The MITRE ATT&CK kill chain is a model where each stage of a cyberattack can be defined, described, and tracked, visualizing each move made by the attacker. Each tactic described within this kill chain has multiple techniques to help an attacker accomplish a specific goal. This framework also has detailed procedures for each technique and catalogs the tools, protocols, and malware strains used in real-world attacks. Consequently, security researchers use these frameworks to understand attack patterns and focus on detecting exposures, evaluating current defenses, and tracking attacker groups.

[15] MITRE's ATT&CK framework catalogs the exact steps and methods used by attackers to exploit a vulnerability.

When we analyzed the 57 vulnerabilities with complete ATT&CK kill chains, we found that 49 CVEs from this subset had already been added to the CISA KEV catalog. In the previous quarterly report, our experts issued specific warnings about the following CVEs: CVE-2017-6884 (QNAP), CVE-2019-2729 (Oracle), and CVE-2020-16875 (Microsoft), which are yet to be added[16] as CISA KEVs. We recommend that CISA add all ransomware-associated vulnerabilities with complete kill chains to its KEV catalog. Further analysis also highlighted that 11 of the 57 kill chain vulnerabilities became associated with ransomware in 2022. This will be another metric we will be tracking every quarter in 2023.

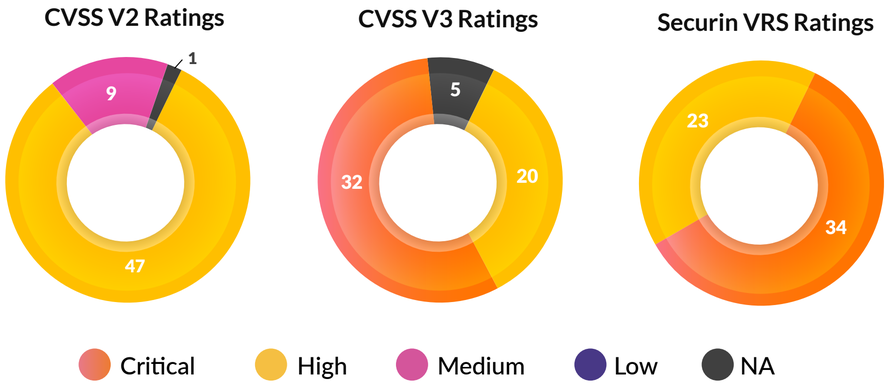
Find out which ransomware-associated vulnerabilities with ATT&CK kill chains are yet to be included in CISA KEVs

VIEW LIST

[16] As of Dec. 15, 2022

Upon assessing what kind of vulnerabilities had a complete kill chain, we found that 25 were old and discovered between 2012 and 2019. The oldest CVEs in this subset were Oracle vulnerabilities: CVE-2012-1710, CVE-2012-1723, and CVE-2012-4681. Next, we examined their severity scores to see how they were rated.

Severity Scores of Kill Chain Vulnerabilities



According to CVSS V2, 47 vulnerabilities were rated high, 9 had a medium severity rating, and 1 CVE had no rating. In CVSS V3, we found 32 vulnerabilities rated as critical, 20 with a high severity rating, and 5 with no rating. Such gaps inhibit security teams from properly prioritizing dangerous vulnerabilities for patches. In comparison, Securin VRS for all 57 kill chain CVEs rated 34 as critical and 23 as high severity, clearly spotlighting the dangerous capabilities of these vulnerabilities.

Next, we examined the exploit type of these vulnerabilities. We found that 34 vulnerabilities (59%) were categorized as Remote Code Execution (RCE) and Privilege Escalation (PE) exploit types—which is not surprising. Interestingly, we also found six vulnerabilities—CVE-2012-1723 (Oracle and 12 other vendors), CVE-2013-0422 (Oracle and eight other vendors), CVE-2019-0708 (Microsoft), CVE-2020-1472 (Microsoft and 17 other vendors), CVE-2021-44228 (Oracle and 19 other vendors), and CVE-2022-29499 (Mitel)—had been trending since December 15, 2022, in the deep and dark web and hacker channels as a point of interest for adversaries.

What makes these vulnerabilities doubly dangerous is the fact that three of them (CVE-2017-18362, CVE-2017-6884, and CVE-2020-36195) are not being detected by the scanners. These vulnerabilities exist in ConnectWise (ManagedITSync), Zyxel (Emg2926 Firmware and Emg2926), and QNAP (QTS' media streaming add-on and multimedia console) and are being exploited by ransomware groups like GandCrab, Ryuk, QNAPCrypt, and Qlocker.

When we analyzed the weakness category of these vulnerabilities, we found five CWEs ranked among the top 10 in MITRE's top 40 dangerous weaknesses (2022).

Top 5 CWEs (with CVEs Having a Complete Kill Chain) in MITRE's Top 10 Dangerous CWEs

CWE-20 has been described as an improper input validation vulnerability and has the maximum number of CVEs categorized within it.

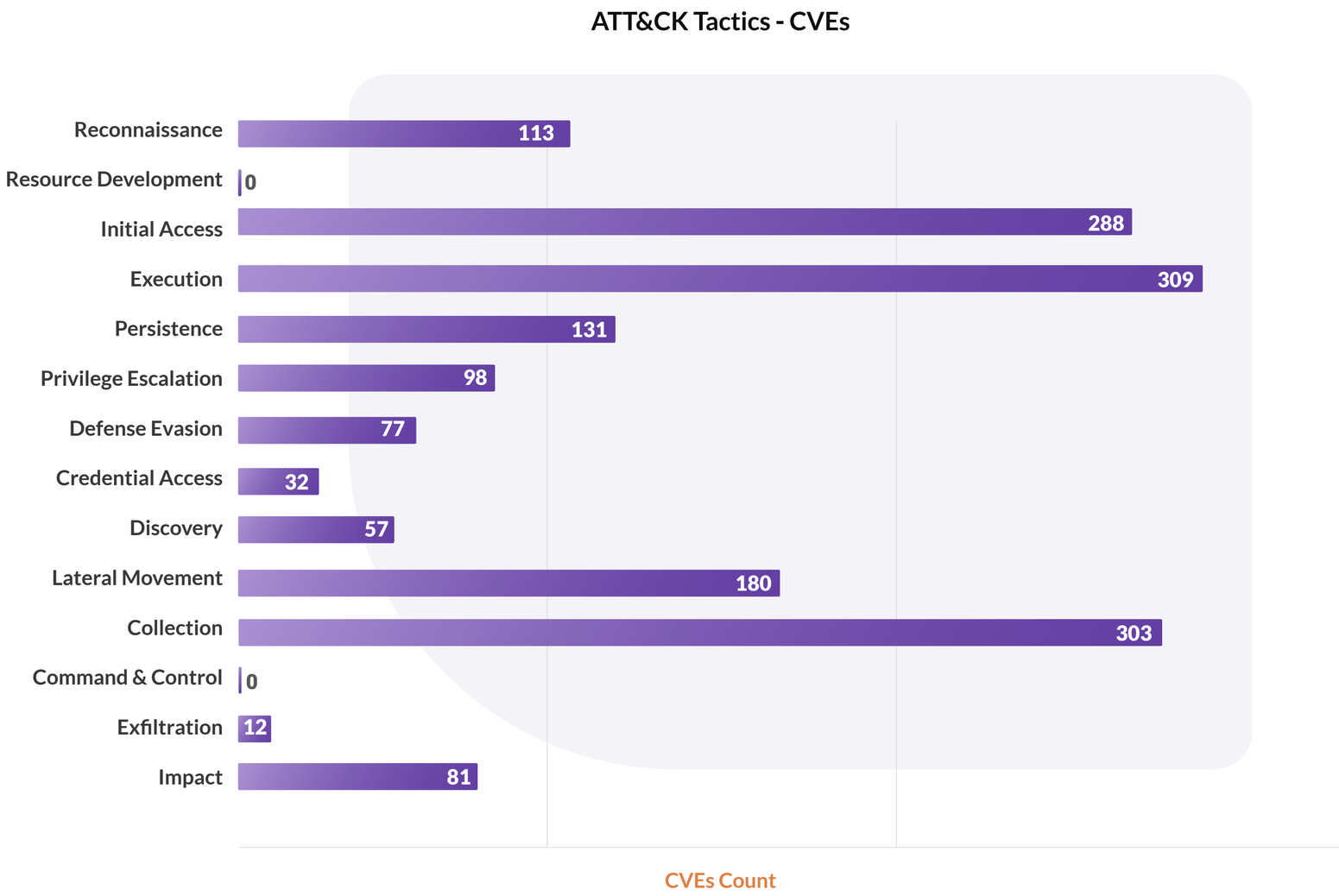
Input validation is a frequently used technique for checking if potentially dangerous input is safe for processing within the code or when communicating with other components. When software does not validate input properly, an attacker can craft input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

These complete takeover vulnerabilities exist in 20 vendors and 81 unique products. Vendors such as Microsoft, Oracle, VMWare, Atlassian, Apache, Pulse Secure, and Sun are vulnerable to these dangerous CVEs. In the past quarter, many products from Oracle have been identified with CVE-2019-2729, a ransomware kill chain vulnerability.

Oracle Products with CVE-2019-2729 (The Kill Chain Vulnerability Added in Q4 2022)

- Identity Manager
- PeopleSoft Enterprise PeopleTools
- Rapid Planning
- Hyperion Infrastructure Technology
- Communications Diameter Signaling Router
- Communications Network Integrity
- Tape Library ACSLS
- StorageTek Tape Analytics SW Tool

MITRE Techniques and Sub-Techniques



On mapping vulnerabilities associated with ransomware to MITRE techniques, we learned that all 344 vulnerabilities combined could easily allow attackers to move across the spectrum of an attack chain. In particular, 299 of these vulnerabilities can be exploited by ransomware groups to enter networks through initial access, 309 vulnerabilities can be exploited to execute custom malware, and 303 can be used to gather sensitive information that can be leveraged to demand ransoms.

Here are a few key observations on the various types of vulnerabilities.

a) Vulnerabilities allowing intruders to enter networks

Services such as external remote services, VPN, and public-facing applications (websites and database [SQL] servers) are commonly used by organizations and contain 133 vulnerabilities associated with ransomware that could be exploited for initial access. Attackers can easily infiltrate vulnerable networks by exploiting these vulnerabilities, breaking the misconception that human interaction is required to execute an attack successfully. To avoid this, organizations need to adopt an environment-aware approach while considering the risk of a vulnerability.

A prominent example of this is the Log4Shell vulnerability (CVE-2021-44228), affecting more than 176 products from 21 vendors and exploited by six ransomware groups, including Conti and AvosLocker. The Confluence RCE vulnerability (CVE-2021-26134) and the recently trending ProxyNotShell vulnerability (CVE-2022-41040 in Microsoft Exchange Server versions) are other examples of vulnerabilities not yet conclusively associated with a ransomware group.

Interestingly, our penetration testers use 10 of the 56 vulnerabilities associated with ransomware added in 2022 as attack vectors for gaining initial access to networks in their penetration testing engagements.

b) Vulnerabilities giving rise to phishing vectors

Phishing is one of the most popular techniques used by attackers to dupe unsuspecting victims into clicking malicious links and attachments or even divulging personal information. Of the 344 vulnerabilities associated with ransomware, we identified a total of 103 vulnerabilities mapped to spear phishing attachment (T1566.001) and spear phishing link (T1566.002) techniques. These vulnerabilities are easy pathways to deliver malicious payloads and provide further motivation for ransomware operators already designing carefully curated and targeted campaigns to attack their victims.

The Follina vulnerability (CVE-2022-30190) affecting 13 products from Microsoft and exploited by the Bisamware ransomware is a classic example of this technique.

Other examples include the Microsoft Office RCE vulnerability (CVE-2017-11882), with seven ransomware groups on its heel, and CVE-2018-20250 (the path traversal vulnerability in RARlab WinRAR), which is associated with four ransomware groups.

c) Vulnerabilities requiring user action

Ransomware operators are constantly looking for specific user actions that they can manipulate. Through social engineering, users may inadvertently execute malicious code by opening harmful email attachments, links, or adversary-placed files, which are in a shared directory or on a user's desktop post initial access.

There are 96 vulnerabilities associated with ransomware that allow such user execution, where attackers rely on victims to open malicious files (T1204.002) and links (T1204.001) to gain elevated access and advanced system control or execute malware. Cyber awareness training for employees and running regular authenticated scans to identify exploited vulnerabilities inside the ecosystem are measures that organizations can adopt to stay safe from such attack methods.

The Follina vulnerability (CVE-2022-30190) is a heavily exploited user execution vulnerability. CVE-2017-0199 (RCE in Microsoft Office) and CVE-2021-26411 (memory corruption vulnerability in Internet Explorer) are other such vulnerabilities users should be wary of.

d) Vulnerabilities providing elevated access

After infiltrating organizational networks, attackers often rely on vulnerabilities that allow privilege escalation to penetrate deeper into the network and execute malware. Our ransomware research identified 75 vulnerabilities with ransomware associations that could enable ransomware actors to elevate privileges (T1608) and easily facilitate lateral movement across organizational domains.

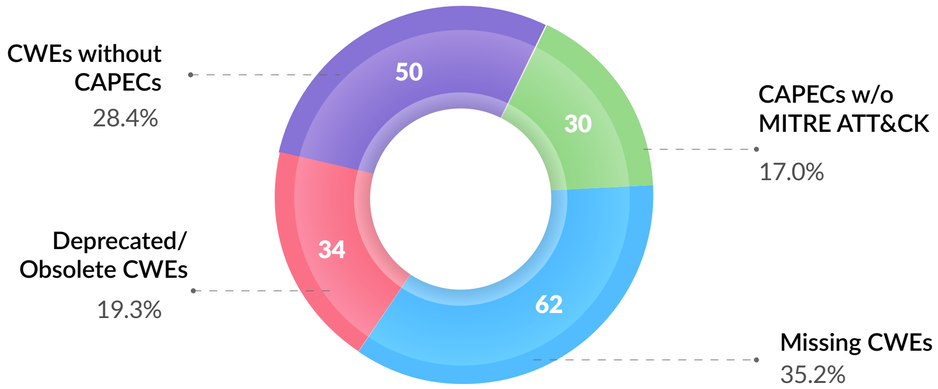
CVE-2021-42278 and CVE-2021-42287 (Active Directory Domain Services Privilege Escalation vulnerabilities), CVE-2022-24521 (Windows CLFS Privilege Escalation vulnerability), and CVE-2021-34523 (Microsoft Exchange Server Elevation of Privilege vulnerability) are good examples of vulnerabilities allowing such elevated privileges.

e) Vulnerabilities allowing stealthy movement

Adversaries use tactics such as disabling security software or blocking script execution to invade and move laterally across vulnerable networks without being identified. Mark-of-the-Web bypass (T1553.005) is a well-known technique used by ransomware operators to abuse specific file formats and override controls. CVE-2022-41091 and CVE-2022-44698 in Microsoft Windows and Server versions are examples.

CVE-2019-16098 gives rise to Bring Your Own Vulnerable Driver issues, where users can use their personal devices rather than an officially allotted device. However, attackers tend to misuse this option to wage attacks and exploit it to evade defense setup (T1211) and impair existing defense practices (T1562.001) by disabling or modifying security tool behavior.

Data Gaps in MITRE Repositories



These gaps are counterproductive for security practitioners and make the organization vulnerable to ransomware and attacks. On average, 17 alternative sources are needed to gather pertinent information about a single vulnerability.

Did you know that security analysts need an average of 17 alternative sources to gather information about a single vulnerability?

Since 2022, our experts have been tracking the gaps in MITRE repositories—an issue that has been a growing inconvenience. For many years, security practitioners have been at a disadvantage due to wrong or old information and missing data in important MITRE repositories, such as the National Vulnerability Database (NVD), Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), and MITRE ATT&CK.

Deprecated CWEs

Overall, eight weaknesses have become obsolete and have not been updated by MITRE; however, we found that 34 vulnerabilities associated with ransomware are still mapped to them. This latency in updating encumbers security researchers trying to understand how dangerous a specific vulnerability is. As a result, researchers are unable to flag the CVE due to a lack of information, which ultimately exposes the organization to ransomware threats.

Obsolete CWE	CWE_Name	Mapped CVEs
CWE-264	Permissions, Privileges, and Access Controls	18
CWE-189	Numeric Errors	6
CWE-399	Resource Management Errors	3
CWE-254	7PK - Security Features	3
CWE-255	Credentials Management Errors	2
CWE-16	Configuration	1
CWE-19	Data Processing Errors	1
CWE-310	Cryptographic Issues	1

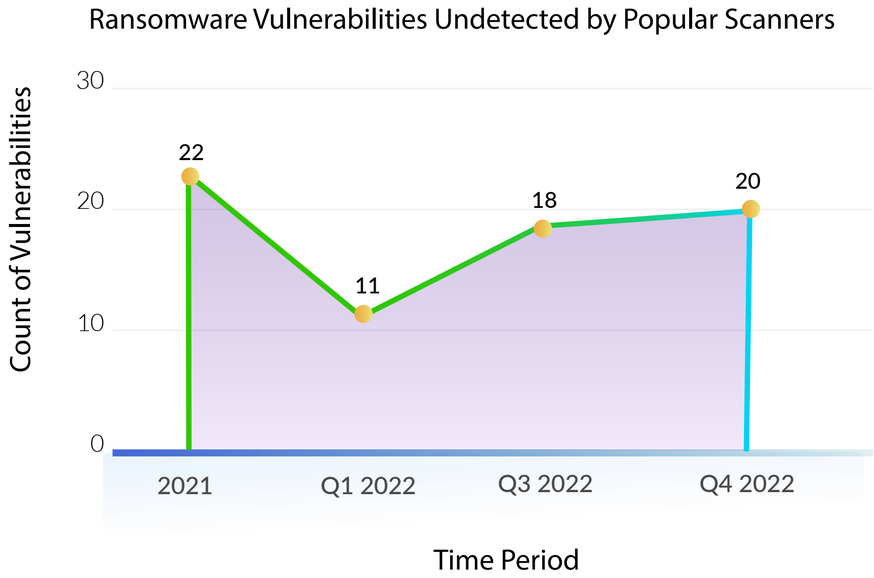
Scanner and Weakness Analysis

Scanners failing to detect the high-risk vulnerabilities being exploited by ransomware is a scary prospect and has security teams rightly worried.

We have been tracking this metric for more than a year; in our last spotlight report (January 2022), we observed that 22 vulnerabilities associated with ransomware remained undetected by scanners. In Q1 2022, this number came down to 11 vulnerabilities, but it rose to 18 vulnerabilities in Q3. Today, there are 20 high-risk vulnerabilities undetected by scanners.

To better understand this blind spot, we analyzed the severity of the 20 undetected vulnerabilities. Although all vulnerabilities associated with ransomware need to be regarded as high risk, we checked the severity of these 20 vulnerabilities based on CVSS V2 and CVSS V3.

We found only nine were rated high in CVSS V2, and six were rated critical in CVSS V3. However, the Securin VRS has marked 16 vulnerabilities as high and 2 as critical.



The low-severity vulnerability, CVE-2013-3993, rated 3.5 in CVSS V2 exists in IBM InfoSphere BigInsights, a business insights platform that analyzes large volumes of data. As this vulnerability is associated with two ransomware gangs (Locky and Petya), it has been given a VRS of 7.34 (high). This comparison shows that, unlike CVSS, Securin VRS computes the accurate threat context of vulnerabilities based on weaponized exploits' trending statistics and potential impact.

Our research also highlights the information gap in the NVD by identifying two vulnerabilities with no severity ratings (CVE-2015-2551 and CVE-2019-9081) that are well associated with ransomware. As both vulnerabilities have been rejected by the NVD with no severity scores or advisories listed, the VRS cannot be calculated despite them being associated with ransomware groups. CVE-2015-2551 is associated with 17 ransomware gangs, notably Cerber, Crypwall, Locky, Reveton, Better_call_saul, and 12 others, while CVE-2019-9081 is tied to two ransomware gangs, Mailto and Satan.

We also observed that four vulnerabilities—CVE-2013-3993, CVE-2017-18362, CVE-2019-16057, and CVE-2019-16920—were part of the CISA KEV catalog with prescribed deadlines for patching. The FCEB and public sector entities were mandated to patch these vulnerabilities within the stipulated deadlines; however, organizations will not know if they are exposed to these CVEs as scanners are not detecting them.

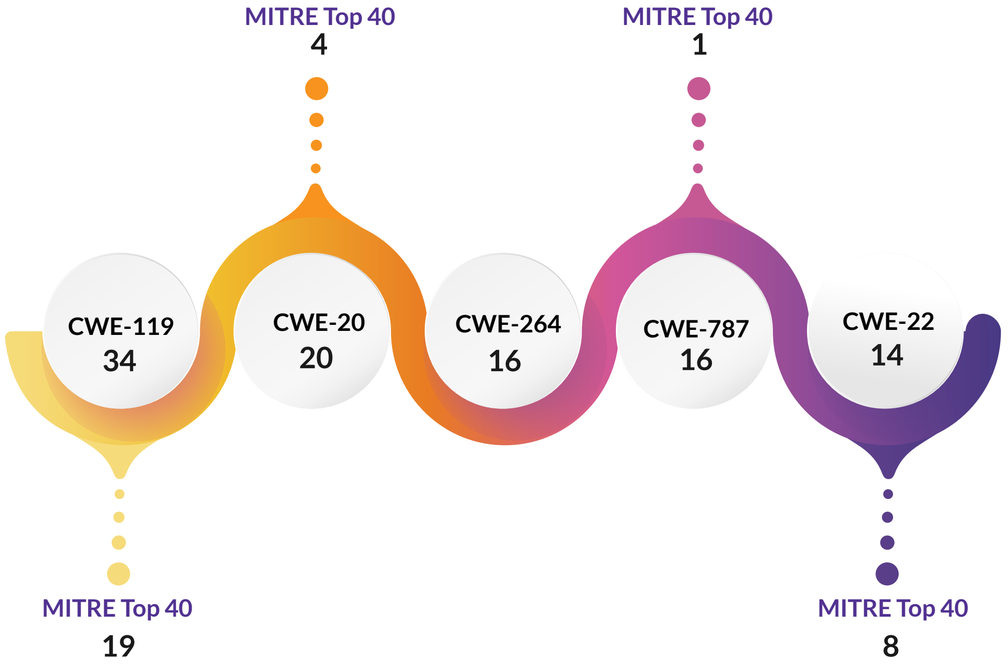
The data gap in the NVD is easily one of the most worrying metrics from our entire investigation, and it ties in with the escalating number of ransomware threats and complex attacks happening worldwide. Weaponizing rejected vulnerabilities makes for a strategic cyberattack. With scanners not detecting them, organizations are at considerable risk unless they augment their countermeasures with a robust attack surface management program.

Get the list of ransomware-associated vulnerabilities undetected by popular scanners **VIEW LIST**

Common weaknesses that contribute to vulnerabilities associated with ransomware

To understand the yearly increase in vulnerabilities associated with ransomware, we analyzed the foundational weaknesses (CWEs)[17] that actively contributed vulnerabilities to this threat. We found that 80 CWEs contributed 344 vulnerabilities to ransomware threats. Among the top five weakness categories with the maximum vulnerabilities linked to ransomware threats, CWE-787 tops MITRE's list for the top 40 most dangerous software weaknesses (2022).

Top Five CWEs Contributing to Vulnerabilities Associated with Ransomware



[17] CWE is a community-developed list of weakness identification, mitigation, and prevention efforts. By mapping the vulnerabilities to CWEs, we can identify a high-level pattern of what kind of weakness is contributing the maximum number of vulnerabilities to ransomware operators and use this information to take preventive measures.

We found 29 weakness categories contributing new vulnerabilities to ransomware threats. In the past quarter, we identified four new CWEs: CWE-125 (Out-of-Bounds Read), CWE-749 (Exposed Dangerous Method or Function), CWE-427 (Uncontrolled Search Path Element), and CWE-674 (Uncontrolled Recursion), which have contributed five vulnerabilities to ransomware threats.

Among the top three weaknesses with the maximum impact, the following CWEs feature on MITRE's top 30 dangerous weaknesses at ranks 5, 18, and 27, respectively.

- CWE-125: Described as an Out-of-Bound Read, this weakness allows attackers to read sensitive information from other memory locations or cause crashes and other unexpected vulnerabilities.
- CWE-306: This weakness is described as Missing Authentication for Critical Function in MITRE. It occurs when the product does not perform any authentication for a function that requires a provable user identity or consumes a significant amount of resources.
- CWE-427: Described as an Uncontrolled-Search-Path Element, this weakness uses a fixed or controlled search path to find resources; however, one or more locations in that path can be under the control of unintended actors.

We also extended MITRE's weakness scoring methodology to vulnerabilities associated with ransomware and scored each weakness based on the CVSS V3 scores of the vulnerabilities under each CWE group and their potential impact.

Based on our analysis, these are the top three weaknesses that promote vulnerabilities associated with ransomware.

CWE ID	CWE Name	Frequency	Score	MITRE 2022 Rank
CWE-119	Improper Restriction of Operations Within the Bounds of a Memory Buffer	39	82.53	19
CWE-20	Improper Input Validation	38	76.28	4
CWE-787	Out-of-Bounds Write	22	43.43	1

Why are these three weaknesses dangerous?

CWE-119 and CWE-787 enable attackers to read and write outside memory buffers, the most popular weakness behind code execution and denial of service (DoS), which are attacker-favorite vulnerabilities. CWE-20 can allow attackers to exploit vulnerabilities in public-facing applications, such as SQL injection and cross-site scripting, which can be easily targeted by malicious actors.

Latency Analysis

Over the last year, we observed attackers weaponizing vulnerabilities at alarming speeds and exploiting them within days of being discovered, sometimes even before the NVD published the information! Latencies in disclosing and delays in the release of patches provide adversaries with a wide window of opportunity to exploit and target organizations unaware of their tech stack's exposure to that particular vulnerability.

We analyzed latencies for the 56 vulnerabilities that became associated with ransomware in 2022 and found that 31 vulnerabilities had been disclosed by their vendors along with patches. When vendors release both the vulnerability's information and patch, hackers lose the opportunity to exploit it unless organizations fail to patch it.

Here are our key findings about vendor latencies:

The NVD: Vendor Latency

With the NVD being one of the most popular and relied-upon sources for vulnerability documentation, we analyzed how attackers utilized delays in vulnerabilities being disclosed for their benefit.

- For 29 vulnerabilities (almost 52%), the vulnerability was added to the NVD after the vendor published it. While the delay spanned from a day to almost a week in most cases, the delay was more than ten days for six vulnerabilities. This shows that there is a window of opportunity of more than a week for malicious actors to mount attacks on organizations that solely depend on the NVD for deciding their patching cadence.

- CVE-2022-26352 in dotCMS was added to the NVD 111 days (over three months) after being disclosed by its vendor.

- A Q4 2022 addition, CVE-2022-36537 in the ZKoss ZK framework, was added to the NVD 844 days after it was disclosed by its vendor, which amounts to almost two years and four months of latency!

- We also noticed how the NVD was ahead in five cases. Specifically, three vulnerabilities in Gigabyte products—CVE-2018-19321, CVE-2018-19322, and CVE-2018-1932. All three CVEs were exploited by the BlackByte ransomware but were added to the NVD in December 2018, more than a year ahead of its disclosure by its vendors (May 2020). Interestingly, the three vulnerabilities saw heavy exploitation much later, in October 2022.

The NVD: Exploit Latency

Now, let us look at how the latency in vulnerabilities being added to the NVD translated to the exploitation of ransomware-associated vulnerabilities in 2022.

- Ten vulnerabilities were exploited even before they could be published on the NVD. This indicates that organizations can be completely exposed to attackers and unaware of dangerous vulnerabilities in their ecosystems.
- Three vulnerabilities were exploited on the same day they were added to the NVD. Organizations that do not have an enumerated view of their attack surface would be in danger, as they would need to move fast and patch on priority.
- There were 29 vulnerabilities listed in the NVD before an exploit code could be added to the public domain. This helped organizations to patch quickly before an exploit could be created. However, adversaries continue to pursue and create exploit codes for any vulnerability that would provide them with an easy path to their target's environment.

Our research indicates that organizations deciding their patching cadence based on the NVD will need to rethink their strategy. The best option is to adopt an ASM solution to scan all assets, including software applications and third-party deployments, and discover the vulnerabilities present across them. However, organizations that need complete coverage should perform a thorough analysis using a vulnerability intelligence platform to analyze vulnerability risks by looking at multiple sources.

Exploit: Patch Latency

Once a vulnerability is exploited by an attacker, it gets on the radar of other threat actors. However, once an exploit code is made publicly available, the vulnerability becomes doubly dangerous, as anyone could readily exploit it. We analyzed the effect of exploits being released in the public domain for vulnerabilities associated with ransomware in 2022.

- Two vulnerabilities, CVE-2022-26134 (in Atlassian Confluence and related products) and CVE-2022-30190 (in Microsoft products), had exploit codes available before they could be patched, with a patch delay of almost two weeks in the case of the latter. This is the riskiest scenario, as exposed organizations that do not adopt alternate mitigation measures will be exposed and defenseless. CVE-2022-26134 is associated with ransomware groups AvosLocker and Cerber, while CVE-2022-30190 is tied to the Bisamware group.

- We also observed that eight of the vulnerabilities associated with ransomware in 2022 were exploited on the same day an official patch was released for the vulnerability. This is an explicit manifestation of the speed at which hackers are weaponizing vulnerabilities today.

- Interestingly, 25 vulnerabilities (almost 45%) were patched before an exploit could be published in the public domain. However, these vulnerabilities are still being exploited and indicate a laxity in the vulnerability management practices adopted by organizations.

Delays and latencies in releasing vulnerability data and patches help adversaries to mount surprise attacks. Additionally, organizations need a deeper understanding of their attack surface to prioritize dangerous vulnerabilities for patching.

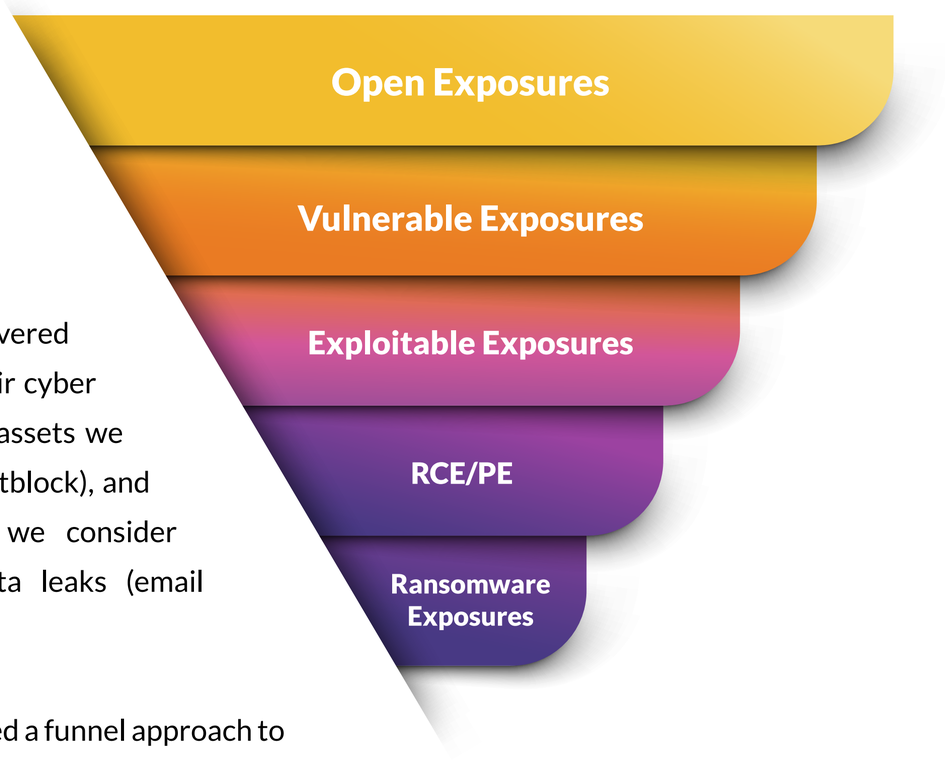
Special Snapshot

Cybersecurity in the US States

An Investigation of the US States' Attack Surfaces

Securin CSW Cyber Security Works ivanti CYWARE™

The Special Snapshot section of this report provides data on the ransomware susceptibility of US state entities. This data was gathered by passively scanning domains belonging to state entities of all 50 states in the US. In this section, we look at the attack surface, region wise, to see what threats might slip through the cracks in their defense.



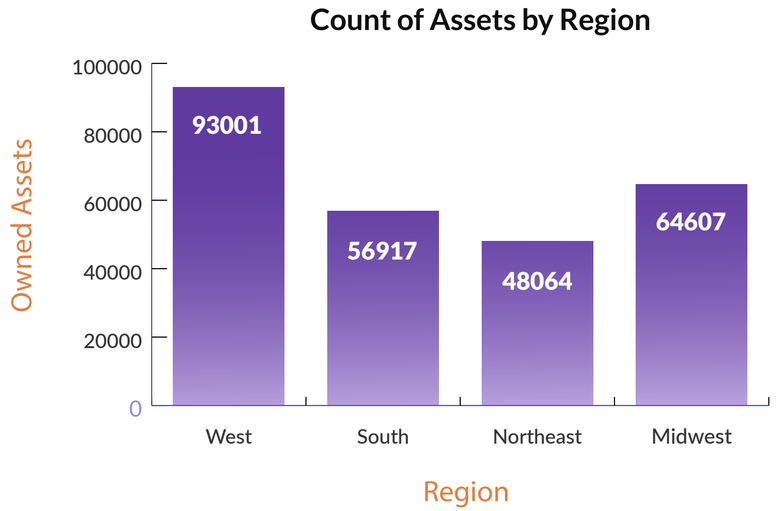
Securin Attack Surface Management (ASM) passively scanned and discovered 262,000 internet-facing assets across 50 US states and investigated their cyber hygiene to understand the potential dangers they are exposed to. The assets we scanned include visible internet hosts, web applications, APIs, CIDR (Netblock), and certificates. While exposure[18] is a broad term, in Securin ASM, we consider misconfigurations (DNS, email servers, hosts, and applications), data leaks (email breaches), and vulnerabilities in products as part of the exposure metric.

Securin ASM analyzed discovered assets, identified exposures, and adopted a funnel approach to prioritize the most dangerous exposures based on the severity, impact, and criticality of assets.

[18] Aggregated number of vulnerabilities on hosts is described as Exposures

Attack Surface by Region

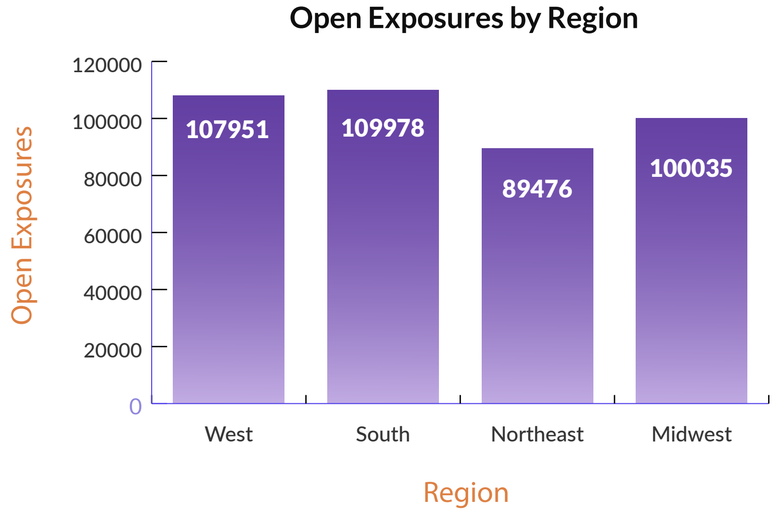
From an asset segregation perspective, the Western region has the biggest attack surface with maximum number of assets, followed by the Midwest. Massive expanding attack surfaces are the crux of the problem for all government entities, as unknown, unmanaged assets within these attack surfaces can invariably expose sensitive data or provide a path for adversaries to infiltrate critical assets.



Open Exposures

Securin ASM considers the following as open exposures: misconfigurations, data leaks, and product vulnerabilities. Open exposures are preferred targets for adversaries as they can be quickly and easily exploited.

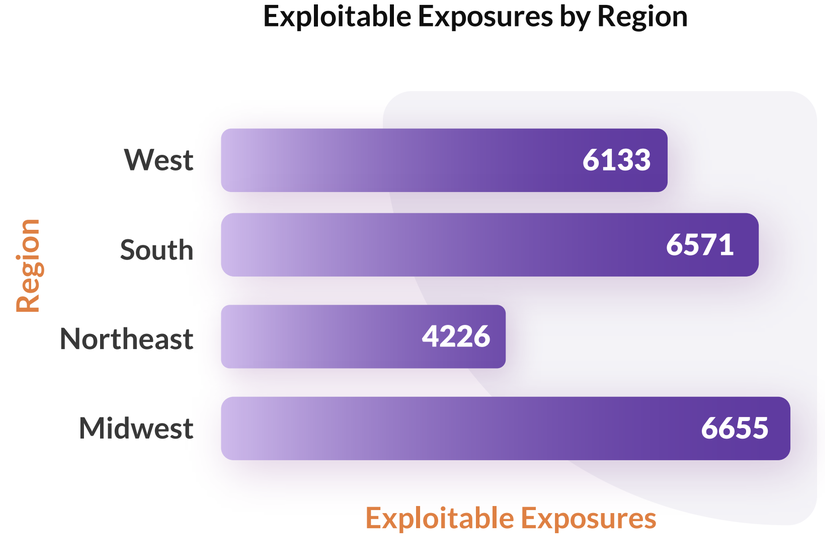
Our analysis found that the Southern states had the maximum open exposures, followed by the West. This spotlights the need for a dedicated discovery engine that would continuously discover known and unknown assets that operate within the expanding attack surface. Unmanaged and unknown assets with dangerous exposures and vulnerabilities are favorite entry points for adversaries to infiltrate and breach.

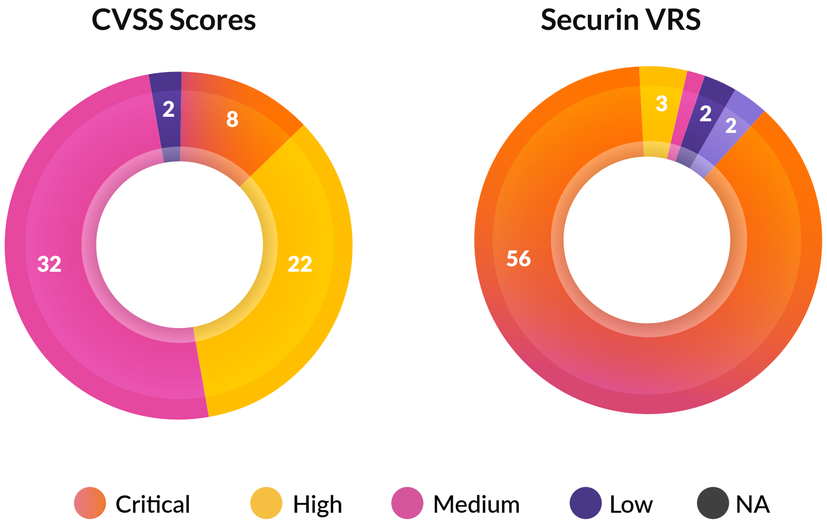


Exploitable Exposures

Exploitable open exposures provide adversaries with more opportunities to maliciously leverage vulnerabilities. We discovered 64 unique vulnerabilities overall in all the states with exploits available in the public domain. We found the Midwest region had more exploitable exposures, followed closely by the South.

An examination of these exploitable CVEs[19] based on CVSS scores[20] showed that 8 were critical and 22 of them were rated high. In contrast, Securin VRS rated 56 as critical and 3 as high.





We also identified two exploitable vulnerabilities, CVE-2019-6111 and CVE-2019-6110, tied to the infamous Ryuk ransomware. Ryuk is notorious for targeting hospitals, especially in 2020, when the world was in the grip of a pandemic. The attacks on US hospitals in California, New York, and Oregon and also in the UK and Germany crippled the healthcare infrastructure and impaired critical care treatments. In the latter part of 2020, a spate of attacks on dozens of US hospitals led to the shutting down of hospitals, as healthcare administrators could not access patient records; it also disrupted chemotherapy treatment for cancer patients in critical condition.

[19] CVEs with public exploits
[20] Securin experts combined CVSS V2 and V3 to have a combined CVSS score for these vulnerabilities

Interestingly, despite this association with this notorious ransomware strain, the CVSS V2 and V3 rate these vulnerabilities as medium severity with scores of 4 and 6.80, respectively, while Securin VRS rates it as a high-severity vulnerability with a score of 7.86. Both vulnerabilities (CVE-2019-6111 and CVE-2019-6110) have been found trending on the internet as a point of interest.

Based on the number of exposures found in the US, the most important question would be whether these regions have visibility into their attack surface. If yes, are they prioritizing the right kind of exposures for remediation?

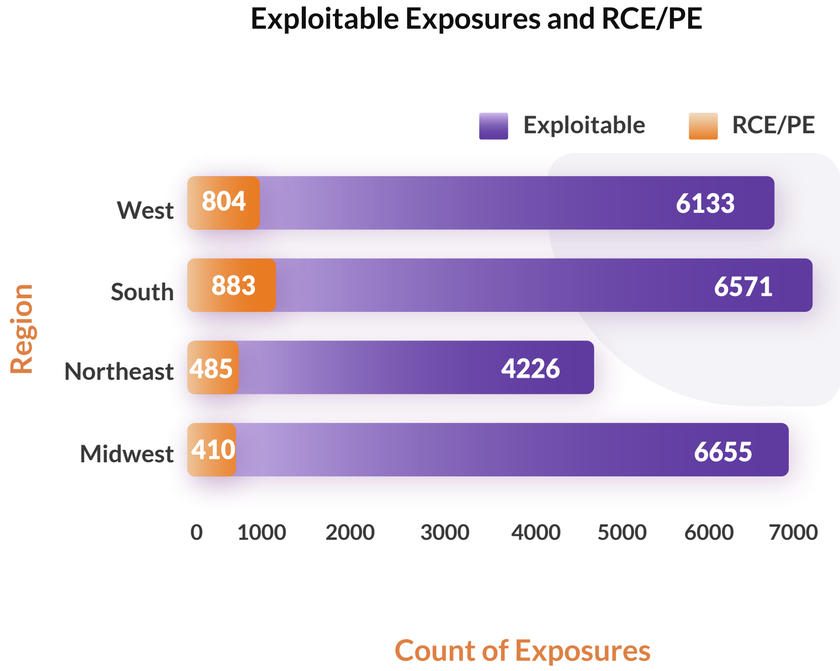
Assets with RCE/PE Exploits

Securin experts prioritize Remote Code Execution and Privilege Escalation (RCE/PE) exploits as the most dangerous vulnerabilities.

The Southern region has the highest number of vulnerabilities classified as RCE/PE exploits, followed by the West. Approximately 13% of exploitable vulnerabilities are RCE/PE, which is a worrying metric.

We have seen increased adoption these exploits by ransomware operators seeking dangerous exploits to compromise exposed assets. The Southern region seems to have more assets exposed to RCE/PE vulnerabilities.

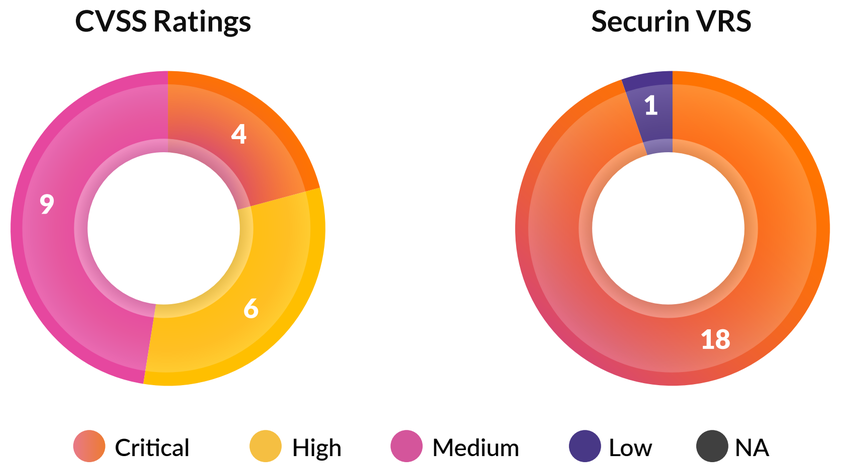
When we examined the susceptibility metric, the South region took the lead with 1.55 exposures per 100 assets, followed by the Northeast region with 1 exposure per 100 assets. From an overall perspective, this is a worrying metric as all US regions have assets with this dangerous exposure.



Our research shows that there are 64 exploitable vulnerabilities in the US, and of them, 19 CVEs have been classified as RCE/PE exploits. We examined their severity ratings and found that four have been rated critical and six as high severity vulnerabilities, but in comparison, VRS rates 18 (out of 19) as critical, because exploitability of the vulnerability is a key scoring factor for Securin VRS..

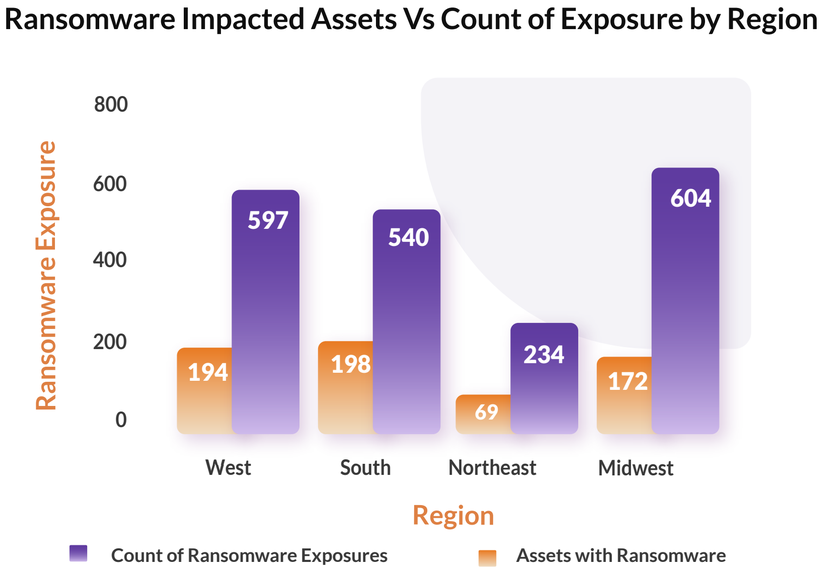
Among the 19 RCE/PE vulnerabilities, our experts highlighted the following vulnerabilities for prioritized patching as they could be exploited on public-facing assets

- CVE-2019-0211 (Apache, Fedora Project, Canonical, Debian, openSUSE)
- CVE-2018-19518 (PHP, Debian, UW IMAP Project, Canonical)
- CVE-2009-2521 (Microsoft)



Assets with Ransomware-Associated Vulnerabilities

We found four CVEs associated with Ryuk ransomware in all the regions. These CVEs exist in the open-source code used in OpenBSD, WinSCP, Canonical, Debian, NetApp, Red Hat, and Oracle products. Unfortunately, this means that all US state agencies using these products are susceptible to ransomware, especially as attackers would only need to exploit one vulnerability associated with ransomware to deploy their malware and cripple computer systems.



The Midwest has the maximum number of ransomware exposures (instances of the affected assets being used within the attack surface), closely followed by the West and the South. In terms of impacted assets, the South is in first place, followed closely by the West. In terms of ransomware susceptibility ratio, the South has 0.94 exposure per 100 assets, followed by the Midwest with 0.93 exposures.

This means that for every 100 assets, one asset is susceptible to ransomware.

The Midwest has the highest number of assets with ransomware-associated vulnerabilities. We also found that one-third of the Midwestern states (4 out of 12 states) have a higher risk of experiencing a ransomware attack as the count of their ransomware exposure is higher than their RCE/PE count.

In comparison, the Northeast has the lowest ransomware exposure and least impacted assets.

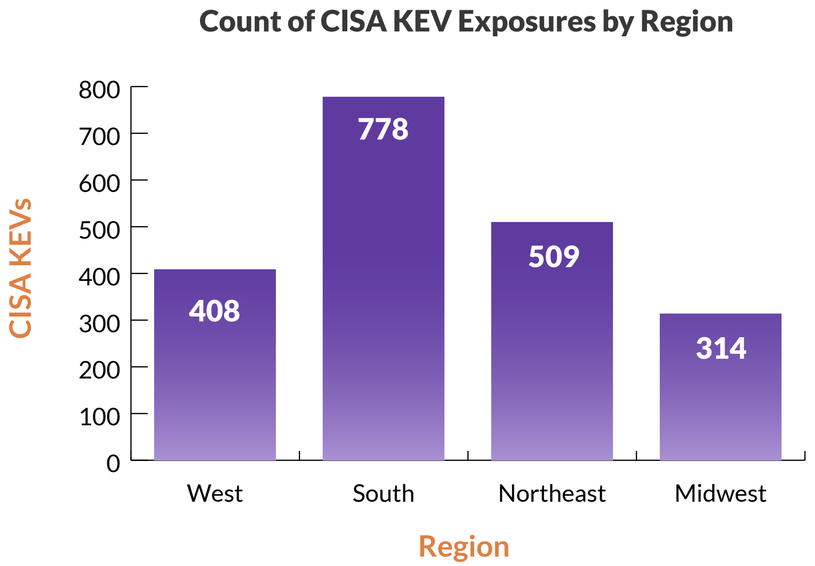
We also identified four ransomware-associated vulnerabilities in all regions, and incidentally, they all are tied to Ryuk ransomware. Interestingly, CVE-2019-6109 and CVE-2018-20685 do not have any publicly known exploits; however, both vulnerabilities are associated with Ryuk ransomware. Securin ASM powered by VRS metrics, takes this threat context into consideration and assigns a higher score to vulnerabilities for their association with Ryuk ransomware despite the lack of publicly known exploits.

CVE ID	Severity Scores	Vendor & Product
CVE-2019-6109	CVSS V2 - 4.00 (Medium) CVSS V3 - 6.80 (Medium) VRS - 7.86 (High)	OpenBSD, WinSCP, Canonical, Debian, NetApp
CVE-2019-6111	CVSS V2 - 5.80 (Medium) CVSS V3 - 5.90 (Medium) VRS - 7.86 (High)	OpenBSD, WinSCP, Canonical, Debian, Red Hat
CVE-2019-6110	CVSS V2 - 4.00 (Medium) CVSS V3 - 6.80 (Medium) VRS - 7.86 (High)	OpenBSD, WinSCP, NetApp
CVE-2018-20685	CVSS V2 - 2.60 (Low) CVSS V3 - 5.30 (Medium) VRS - 7.66 (High)	OpenBSD, WinSCP, NetApp, Debian, Canonical, Red Hat, Oracle

Assets with ransomware-associated vulnerabilities can put an entire state's machinery and infrastructure at high risk. Unless the government entities in all the regions have a greater visibility into their attack surface and the assets that operate within, they are at risk of becoming the next ransomware victim. To protect an ever-expanding attack surface, organizations need a robust ASM solution that will continuously prioritize exposures and help remediate them. Automated discovery of all assets and continuous asset monitoring based on criticality, impact, exploits, and threat associations is the need of the hour for these regions.

CISA Known Exploited Vulnerabilities

CISA has mandated Federal Civilian Executive Branch (FCEB) entities to remediate all Known Exploited Vulnerabilities (KEVs) within stipulated deadlines. The KEV catalog is a dynamic list of vulnerabilities that have been exploited in the past or present; it presents clear remediation guidelines allowing organizations to patch without any complication. CISA has been updating the KEV catalog with the trending list of CVEs that can cause immediate harm. However, as CVSS scores are unreliable and NVD and MITRE latencies have been enabling adversaries, the CISA KEV catalog is the best option for organizations to kick-start their vulnerability prioritization framework.

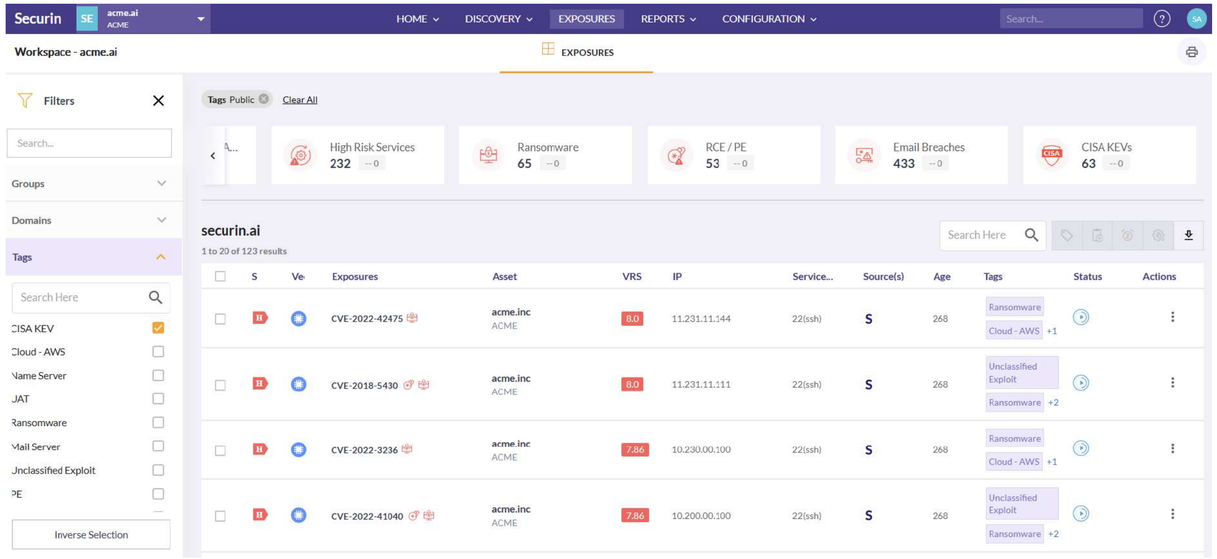


We found five CISA KEV exposures in all US regions. The South has the highest CISA KEV exposures followed by the Northeast. Unfortunately, the deadlines for patching these KEVs have already lapsed.

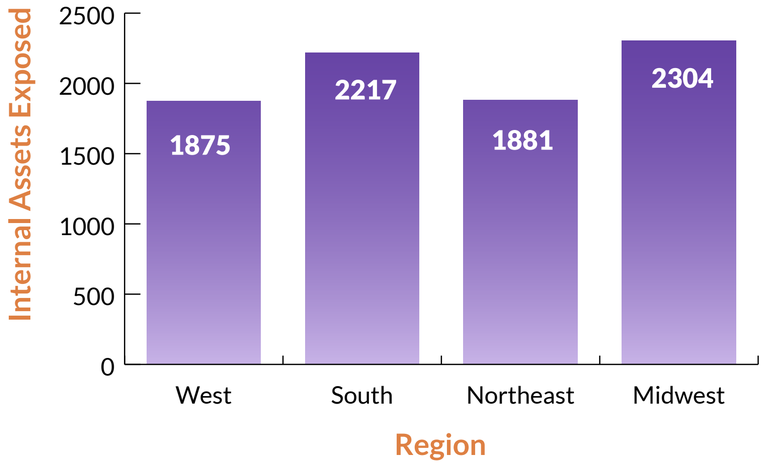
CVE ID	Vendor & Product	Deadline
CVE-2019-0211	Apache, Fedora Project, Canonical, Debian, openSUSE	May 3, 2022
CVE-2020-36193	PHP, Fedora Project, Debian, Drupal	Sep 15, 2022
CVE-2020-13671	Drupal, Fedora Project	Aug 18, 2022
CVE-2020-28949	PHP, Debian, Fedora Project, Drupal	Sep 15, 2022
CVE-2021-40438	Apache, Fedora Project, Debian, NetApp, F5, Oracle, Siemens	Dec 15, 2022

For government entities, remediating CISA KEVs should be a no-brainer. The catalog provides prescribed deadlines by which these vulnerabilities need to be remediated. Furthermore, as these KEVs have clear remediation guidance with patch availability, it should be an easy exercise for US state entities to patch them, unless they are unaware of these exposures.

Securin ASM with the CISA KEV Filter



Internal Assets Exposed by Region

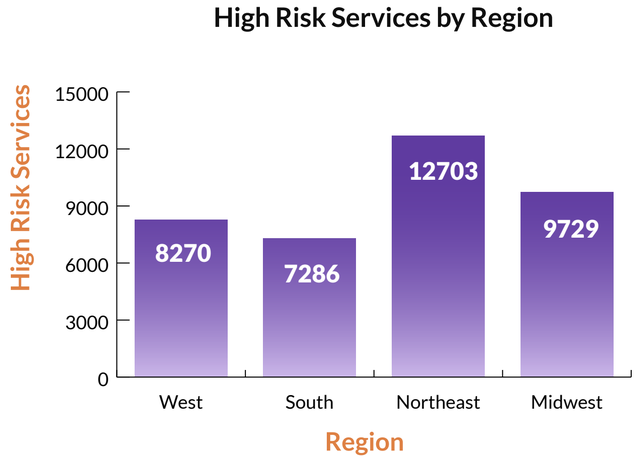


Exposed Internal Assets

Yet another common attack vector that puts organizations at high risk is non-production environments and internal IPs exposed to the internet. Internal IPs and test environments must be used internally, but hackers can use leaked test credentials to log into these environments and access massive volumes of customer data. The Midwest has the highest internal assets exposed to the internet, followed closely by the South.

High-Risk Services

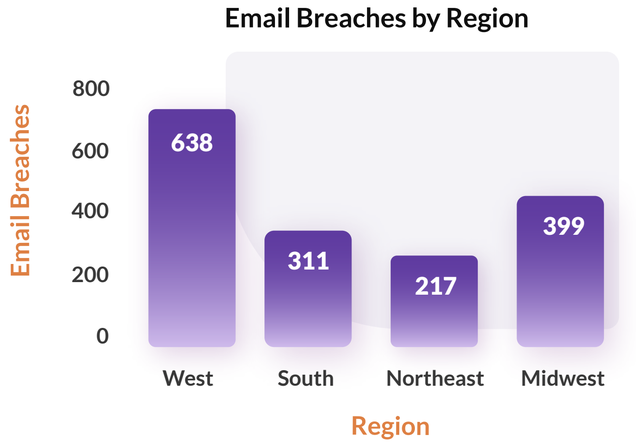
When we analyzed the services running within each region, the Northeast region had the most high-risk services, followed by the Midwest. High-risk services are unsafe services with ports open to the public internet; they lack sufficient network security and are easily exploited by attackers. These services can also be third-party associations and cloud platforms.



Email Breaches by Region

The exposure of email IDs in a breach is a significant security risk, as it paves the way for phishing, internal sabotage, and fraud attacks. Our analysis found that the Western region had the maximum email addresses exposed in breaches, with 638 email credentials available in the deep and dark web. This makes it extremely easy for an attacker to gain unauthorized access and move laterally within the environment, and access assets with sensitive information.

Based on these passive scans, the Southern region seems to be most vulnerable with the highest open exposures, exploitable exposures, and RCE/PE exploits; it also has the most assets with ransomware-associated vulnerabilities and the highest unpatched exposures to KEVs.



Based on our analysis, our experts have prioritized the top 10 vulnerabilities found in all the US State regions that need to be prioritized for patching immediately.

Top 10 vulnerabilities that US States need to remediate immediately! VIEW LIST

Overall, the US regions need better visibility into their attack surface, followed by continuous remediation of key exposures. These key exposures need to be prioritized by the impact and criticality of the asset so that agencies can remediate the most dangerous exposures first. Adopting automated solutions to continuously monitor and discover unknown assets will help shrink these attack surfaces. Any state entities that run their vulnerability management program based on CVSS ratings will be severely disadvantaged. As the CISA KEV catalog does not yet list all the vulnerabilities associated with ransomware, US state entities may need to augment their vulnerability management program with an accurate vulnerability intelligence feed and a contextualized scoring system to help vulnerable regions gain resilience against adversaries.

Predictive Insights

Securin | CSW Cyber SecurityWorks | ivanti | CYWARE™

Predictive Insights

Top vulnerabilities that may be exploited in the future

As always, our Securin experts conduct an in-depth analysis to bring you early warning alerts about vulnerabilities that could be exploited in the future. Our predictive scores based on AI and ML models (ranging from 1 to 38.46) rise high whenever a vulnerability is discussed in hacker channels, on the news or social media, or is exploited in the wild. The higher the predictive score, the more likely it is that the vulnerability will be exploited by attackers in the near future. These scores serve as a warning to users of the Securin VI platform.

Trending Vulnerabilities

CVE ID	Vendor-Product	D-VRS	P-VRS	CISA KEV
CVE-2022-41082	Microsoft Exchange Server	9.58	38.46	Yes
CVE-2022-41040	Microsoft Exchange Server	9.31	38.46	Yes
CVE-2022-41080	Microsoft Exchange Server	8.79	38.46	Yes
CVE-2022-30190	Microsoft Windows and Server versions	9.22	38.46	Yes

Exploitable Vulnerabilities on Public-Facing Assets

CVE ID	Vendor-Product	D-VRS	P-VRS	CISA KEV
CVE-2022-47523	Zoho Corp ManageEngine-related products	6.80	31.39	No
CVE-2022-43931	Synology VPN Plus Server	6.28	26.22	No
CVE-2022-27518	Citrix Application Delivery Controller Firmware and Gateway Firmware	8.79	38.46	Yes
CVE-2022-40684	Fortinet FortiSwitch Manager, FortiProxy, and FortiOS	9.38	38.46	Yes
CVE-2022-41622	F5 Big IP-related products	9.07	7.58	No

Perennial Favorites

CVE ID	Vendor-Product	D-VRS	P-VRS	CISA KEV
CVE-2021-44228	21 vendors and 176 products	9.98	38.46	Yes
CVE-2021-34473	Microsoft Exchange Server	9.96	38.46	Yes
CVE-2021-34523	Microsoft Exchange Server	9.96	38.46	Yes
CVE-2021-31207	Microsoft Exchange Server	9.96	38.46	Yes
CVE-2021-26855	Microsoft Exchange Server	9.96	38.46	Yes
CVE-2021-27065	Microsoft Exchange Server	9.22	38.46	Yes

Noteworthy Trends and Interesting Facts

The most popular **initial access vectors** in 2022 were phishing, email compromise, stolen credentials, and vulnerabilities. Furthermore, the **exploitation of vulnerabilities** by ransomware groups has **accelerated** compared to 2021, calling for an immediate need for good vulnerability management practices across the board.

Attackers targeting **zero-day vulnerabilities** is an ongoing trend that we had observed since publishing our Ransomware Reports in 2021. This trend continued to grow in 2022 with vulnerabilities being rapidly exploited even before an official patch could be released. We illustrate three such CVEs that had ransomware associations emerging recently.

Malware with **cross-platform capabilities** is in high demand, as ransomware operators can easily target multiple operating systems via a single codebase—some players being the Black Basta and Luna ransomware. Attackers also use ransomware specially designed for Linux owing to the advanced root-level capabilities such code offers.

The **triple extortion** technique, although rarely used due to the cost and complexity involved, had its traces in 2022 with instances of the LockBit gang adopting the method. The Avaddon group and REvil gang are other adopters of the method.

Another interesting trend is the rise in ransomware groups' adoption of the wiper functionality. The wiper code allows groups to delete or destroy an organization's data rather than merely encrypt it. Groups like BlackCat have taken to this tactic, which was also popular in the Iran-Albania cyberwar. We have also observed instances where **malware loaders were used for initial access**, followed by **ransomware code execution** at a later stage.

We also observed a significant number of **attacks on third-party providers of security solutions**, such as identity access management or device management, as was the case with **cryptocurrency attacks.** Interestingly, software code libraries like PyPi and GitLab repositories were also highly targeted by attackers, opening the doors to a plethora of possible victims. There were also instances of ransomware code lurking in open source packages like npm.

It is also worth noting the role of the FBI, CISA, and cybersecurity governing bodies that have stepped up their efforts to combat ransomware threats and successfully recovered ransom payments in multiple instances.

Interesting Infobytes

- **Is bug bounty only for the good folks? Not the case anymore!**

  The LockBit ransomware group introduced the first known ransomware bug bounty program for identifying bugs. The program paid rewards between $1000 to $1 million to bounty hunters in return for flagging flaws while also encouraging innovative ideas for improving their ransomware program.

- **Development in all walks of life**

  Ransomware groups are turning to the Rust or Go (aka Golang) languages owing to the former's stability and integration capabilities and the latter's cross-flexibility.

- **Extent of organization in RaaS forums**

  With interviews and data leaks emerging about the LockBit and Conti gangs, the organized mode of operations of these Ransomware-As-A-Service (RaaS) offerings came as a surprise. It suggested that RaaS groups functioned similarly to a regular IT company, complete with employee designations, hierarchy, and even payroll options.

- **Ransomware leaks and DDoS attacks**

  In the latter half of 2022, the LockBit 3.0 group suffered a leak of its builder code when an angry developer put it up for sale online. The builder was subsequently used by another group, Bloody ransomware. In other news related to ransomware groups, many groups have recently had their leak sites hit by DDoS attacks, leading to downtime and outages.

Attackers and the Attacked

We witnessed ransomware groups repeatedly waging attacks on unsuspecting victims throughout our research in 2022. BlackCat/AlphaV, LockBit, Vice Society, **Hive**, and **AvosLocker** groups were the most prevalent of the lot—waging attacks, leaking victims' information, and adopting advanced tactics in their attacks. The **Black Basta** and **Cl0p** groups are other notable mentions. The FBI has also warned against Maui and MedusaLocker groups.

There were also instances of **multiple ransomware groups simultaneously waging attacks on a single victim**. While we may not be able to confirm if the attacks were planned or coincidental, it is clear that ransomware groups work in tandem, definitely when it comes to sharing exploit codes, attack methods, ransom note elements, and even victim-specific information under the broader category of affiliates.

Additionally, the PrintNightmare vulnerability that we disclosed as associated with ransomware in Q3'21 continued to trend in 2022, with four ransomware groups developing the capability to exploit the vulnerability: Conti, Cerber, Vice Society, and Black Basta.

The healthcare **sector**, (which we covered in Special Snapshot in the Q1'22 report) continued to see an increase in attacks throughout the year. Schools and **government offices** followed suit. The intriguing aspect was the increased attention garnered by the **automotive and transportation sectors**, with manufacturers and service providers targeted in multiple cyberattacks.

Storage devices continued to bear the brunt of cyberattacks in 2022, a trend we have been observing since 2021. Ransomware groups like Checkmate and NamPoHyu (MegaLocker) have now joined the fray along with Qlocker, eCh0raix, and Deadbolt groups.

Future Predictions

What does the future hold for us? Having researched the threat world for decades now, our researchers call out some trends we might expect in the future.

- The democratization of AI is enabling hackers to become more sophisticated. For instance, software like the chatbot, ChatGPT, helps newbie threat actors to write exploits; there are no regulations for such AI-based tools and its potential remains unchecked.
- Public sector infrastructure will be in the sniper scope of threat actors with targeted ransomware attacks, of which software supply-chain exploitation will be the key accelerator.
- Threat actors will evolve novel techniques with an emphasis on gaining initial access and subsequent defense evasion.

Conclusion

Ransomware has become an escalating and evolving threat that can destroy a country's infrastructure or be deployed as a weapon of choice by adversaries to cripple an enemy nation. Adversaries are continuously adding more potent vulnerabilities to the ransomware arsenal. Rejected vulnerabilities, low-scoring CVEs, and old resurrected vulnerabilities are being weaponized so that they can slip through the cracks of an organization's defense.

One of the many things discovered during our research in the past year is that security teams have been fighting this menace with a blindfold on their eyes in addition to their hands tied behind their backs. It is no wonder that adversaries are winning this game. Most data repositories, NVD, and MITRE, have gaping information holes inhibiting our security teams from getting the true picture of such threats. The Common Vulnerability Scoring System (CVSS) is not giving the true threat context of vulnerabilities, further hindering our security teams from prioritizing them. Even the CISA KEV catalog, an otherwise valuable initiative, has gaps in its list and is missing many critical CVEs. Our investigation into the cyber hygiene of the US state agencies spotlights the lack of visibility in their attack surface, making it easy for adversaries to plan and attack their targets.

The threat landscape is evolving every second and organizations cannot afford to remain passive anymore. Adversaries are becoming more sophisticated and are expanding their targets to cause more disruption and destroy critical infrastructure. It is time to help security teams with automated solutions to prioritize

"This report highlights the increasing danger and sophistication of ransomware attacks, which have the potential to cause significant damage to individuals, organizations, and even entire countries. Adversaries are leveraging a variety of techniques, including weaponizing previously rejected vulnerabilities, low-scoring CVEs, and older vulnerabilities that have been resurrected, to evade detection and infiltrate organizations. This report emphasizes the need for organizations to stay vigilant and prioritize vulnerabilities based on risk factors, threat associations, exploitability, and criticality in order to minimize the risk of a ransomware attack."

- Aaron Sandeen,
Founder and CEO, Cyber Security Works and Securin

"It is an unfortunate reality that ransomware remains a threat to organizations of all sizes and we will continue to see ransomware evolve and extend to data modification and destruction. Ransomware attacks are becoming increasingly common, with more than 4,000 attacks happening every day. We expect that this number will only go up as threat actors continue to access more sophisticated tools to launch their attacks, such as Generative AI which will make it possible to launch attacks at machine speed. With the threat landscape currently tilted heavily in favor of threat actors, it is vital for organizations to have a comprehensive security solution in place that can detect and prevent these attacks. By leveraging the information in this report, and implementing a risk-based vulnerability management solution, organizations can finally begin to go on the offensive with their cyber strategy."

- Srinivas Mukkamala,
Chief Product Officer at Ivanti

"Over the last year, ransomware remained one of the top threats that organizations faced. Adversaries expanded their targets to software supply chains and have had measurable impacts on business operations downstream. The information gaps in threat intelligence and internal silos often inhibit security teams from getting ahead of such threats. Organizations need to prioritize automated solutions for their security teams to leverage threat intelligence and initiate proactive responses. While adversaries continue to craft stealthy tooling, techniques, and tactics, to weaponize vulnerabilities, it is essential for SecOps teams to automate and orchestrate their processes to mitigate risk through real-time operationalization."

- Anuj Goel,
Co-founder & CEO, Cyware

About Us

Securin

Securin is obsessed with helping leaders continuously improve their security posture. We partner with our customers using our tech-enabled services including Attack Surface Management, Vulnerability Management, Pentesting and Vulnerability Intelligence. As a US Department of Homeland Security sponsored CVE number authority (CNA), we have deep expertise in offensive pentesting and unique insights into the latest threats. Our capabilities allow us to continuously reduce your attack surface and provide predictive intelligence, so you can stay ahead of the bad actors. At Securin, we work as an extension of your team, providing the glue to create a security fabric that protects your organization.

For more information, visit www.securin.io and follow us on LinkedIn and Twitter.

CSW Cyber SecurityWorks

For more than a decade, CSW's vulnerability and exposure management solutions have helped clients across different geographies to secure their enterprises from emerging cyber threats. Our vulnerability and exposure management solutions have secured the IT infrastructure of diverse verticals in government entities, IT infrastructure, and private clients and have improved their security posture.

CSW is a US Department of Homeland Security–sponsored CVE Numbering Authority whose exploit research has led us to discover 54+ zero days in popular products such as Oracle, D-Link, WSO2, Thembay, and Zoho.

For more information, visit www.cybersecurityworks.com and follow us on LinkedIn and Twitter.

ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they can work from anywhere. The Ivanti Neurons automation platform connects the company's industry-leading unified endpoint management, cybersecurity, and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and empowers users to self-service. Ivanti manages over 200 million devices for 40,000+ customers, including 96 of the Fortune 100. Customers have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge and deliver excellent end-user experiences for employees, wherever and however they work.

For more information, visit www.ivanti.com and follow us on LinkedIn and Twitter.

CYWARE™

Cyware helps enterprise cybersecurity teams build platform-agnostic virtual cyber fusion centers. Cyware is transforming security operations by delivering the cybersecurity industry's only Virtual Cyber Fusion Center Platform with next-generation security orchestration, automation, and response (SOAR) technology. As a result, organizations can increase speed and accuracy while reducing costs and analysts' burnout. Cyware's Virtual Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, information sharing groups (information sharing and analysis centers and information sharing and analysis organizations), managed security services providers, and governmental agencies of all sizes and needs.

For more information, visit www.cyware.com and follow us on LinkedIn and Twitter.

Appendix 1

Top vulnerabilities associated with ransomware to be included in CISA KEV

CVE ID	Vendor & Product	Ransomware Association
CVE-2013-4786	Oracle (Fujitsu M10 Firmware) Intel (Intelligent Platform Management Interface)	HPE iLO
CVE-2017-12542	HP (Integrated Lights-Out 4 Firmware)	HPE iLO
CVE-2017-7494	Samba (Samba) Debian (Debian_linux)	Decryptiomega, QNAPCrypt, StorageCrypter, NamPoHyu
CVE-2021-44832	Apache (Log4J) Novell (openSUSE) Red Hat (Enterprise Linux) Cisco (CloudCenter) Oracle (26 products) Fedora Project (Fedora) Debian (Debian Linux) Nutanix (AOS) Amazon (Linux)	AvosLocker
CVE-2021-45046	Apache (Log4j) Intel (9 products) Siemens (60 products) NetApp (7 products) Splunk (Splunk) Red Hat (Enterprise Linux) Palo Alto Networks (Pan-OS) Nutanix (AOS) Novell (openSUSE) FreeBSD (FreeBSD) Canonical (Ubuntu Linux) Aruba Networks (Silver Peak Orchestrator) Amazon (Linux) Debian (Debian Linux) SonicWall (Email Security) Fedora Project (Fedora)	AvosLocker
CVE-2021-45105	Apache (Log4j) NetApp (Cloud Manager) SonicWall (13 products) Oracle (106 products) Amazon (Linux) Canonical (Ubuntu Linux) Debian (Debian Linux) FreeBSD (FreeBSD) Novell (openSUSE) Nutanix (AOS) Red Hat (Enterprise Linux)	AvosLocker
CVE-2019-16098	MSI (Afterburner)	BlackByte

Appendix 2

Eight CVEs with complete MITRE ATT&CK Kill Chain yet to be prioritized by CISA

CVE ID	Vendor & Product	Ransomware Association
CVE-2016-10401	Zyxel PK5001Z and firmware	Stop
CVE-2017-6884	Zyxel EMG2926 and firmware	Ryuk
CVE-2018-8389	Microsoft (12 products)	Ryuk
CVE-2019-2729	Oracle (11 products)	Sodinokibi
CVE-2020-1210	Microsoft SharePoint and related products	Zeppelin
CVE-2020-16875	Microsoft Exchange Server	Zeppelin
CVE-2020-36195	QNAP (3 products)	QNAPCrypt and Qlocker
CVE-2021-31206	Microsoft Exchange Server	AvosLocker

Appendix 3

Ransomware CVEs missed by popular scanners (Nessus, Nexpose, and Qualys)

CVE ID	Vendor	Product	Ransomware Family Associations	Patch Links	CISA KEV: Y/N
CVE-2010-1592	SiSoftware	Sandra	Robinhood	Information not available	No
CVE-2012-3347	EFS Technology	AutoFORM PDM Archive	Crypsam (SamSam)	1, 2, and 3	No
CVE-2013-0322	2 vendors	2 products	32 groups	1 and 2	No
CVE-2013-2618	Network Weathermap	Network Weathermap	Ryuk	Patch Now	No
CVE-2013-3993	IBM	InfoSphere BigInsights	Locky and Petya	Patch Now	Yes
CVE-2015-2551	Information not available	Information not available	17 groups	Information not available	No
CVE-2015-7465	IBM	Jazz Reporting Service	Cerber	Patch Now	No
CVE-2017-15302	CPUID	CPU-Z	Robinhood	Patch Now	No
CVE-2017-18362	ConnectWise	ManagedITSync	GandCrab	1, 2, and 3	Yes

CVE ID	Vendor	Product	Ransomware Family Associations	Patch Links	CISA KEV: Y/N
CVE-2017-3197	Gigabyte	4 products	UEFI	1, 2, and 3	No
CVE-2017-3198	Gigabyte	4 products	UEFI	1, 2, and 3	No
CVE-2017-6884	Zyxel	2 products	Ryuk	Information not available	No
CVE-2019-16057	D-Link	2 products	Cr1ptT0r	Patch Now	Yes
CVE-2019-16647	2 vendors	2 products	BitPaymer	Patch Now	No
CVE-2019-16920	D-Link	8 products	Cyborg	EOL	Yes
CVE-2019-5039	OpenWeave	OpenWeave Core	ASN.1	Patch Now	No
CVE-2019-9081	Laravel	Framework	Mailto and Satan	Patch Now	No
CVE-2020-36195	QNAP	3 products	QNAPCrypt and Qlocker	Patch Now	No
CVE-2021-33558	Boa	Boa	Hive	EOL	No
CVE-2022-36537	zkoss	ZK Framework	LockBit	Patch Now	No

Appendix 4

Top 10 vulnerabilities that the US states need to remediate immediately

CVE ID	Vendor/Product	Threat Association	CISA KEV Y/N
CVE-2019-0211	Apache, Fedora Project, Canonical, Debian, openSUSE	Ryuk	Yes
CVE-2020-36193	PHP, Fedora Project, Debian, Drupal		Yes
CVE-2019-6111	OpenBSD, WinSCP, Canonical, Debian, Red Hat		No
CVE-2020-28949	PHP, Debian, Fedora Project, Drupal		Yes
CVE-2020-13671	Drupal, Fedora Project		Yes
CVE-2018-19518	PHP, Debian, Uw Imap Project, Canonical		No
CVE-2009-2521	Microsoft		No
CVE-2017-9798	Apache, Debian		No
CVE-2021-40438	Apache, Fedora Project, Debian, NetApp, F 5, Oracle, Siemens		Yes
CVE-2016-0736	Apache		No