CSW Cyber SecurityWorks

Securin

Decoding CISA KEV

An Annual Review of CISA's Known Exploited Vulnerabilities (KEV)

KEV Metrics & Threat Associations

2021-2022

CISA's KEVs— An Introduction

A year ago, on November 03, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) published a living list of vulnerabilities called Known Exploited Vulnerabilities (KEVs) to help the Federal Civilian Executive Branch (FCEB) and other public sector organizations to remediate frequently exploited vulnerabilities, reduce the risk of cyberattacks, and strengthen their security posture.

Within a year of its launch, CISA's KEV Catalog has become an authoritative repository of information based on which organizations can start their vulnerability management efforts; for public sector companies and entities, it has become an integral part of the top vulnerability prioritization layer.

By initiating this exercise, CISA has sent a clear message to organizations to prioritize vulnerabilities that adversaries exploit to mount crippling cyberattacks. The goal behind this remediation drive is to reduce risk, help organizations manage their vulnerabilities in a better way, and keep pace with the evolving threat activity.

While CISA's KEV Catalog is a valuable resource as a repository of vulnerabilities to be patched, it does not give any threat context to help the FCEB and public sector organizations to understand why they should be patching them.

Through Decoding CISA KEV reports, CSW experts take a step back to provide a holistic view of the KEV Catalog and its vulnerabilities to understand what types of vulnerabilities are being added to this list and to bring forward the threat context associated with each vulnerability. Our deep dive into the KEV Catalog provided public sector organizations with invaluable information to aid them in their remediation efforts.

In many instances, we also found that our early warning alerts about certain vulnerabilities have been added to the KEV Catalog, reaffirming our research.

Report Methodology

This report has been put together using CISA's KEV Catalog and the month-on-month analysis that CSW's researchers have delivered to our customers for the past year. Our researchers used the NVD, MITRE, and other repositories to map each vulnerability to Tactics, Techniques, and Procedures (TTPs) to understand the actual risk posed by these vulnerabilities. We cross-referenced the KEVs with our ransomware and threat groups' database maintained in Securin Vulnerability Intelligence (VI) to provide additional threat context to the KEV Catalog. We have also used our proprietary threat intelligence platform (Securin VI) to predict and recommend vulnerabilities that need to be a part of the KEV Catalog.

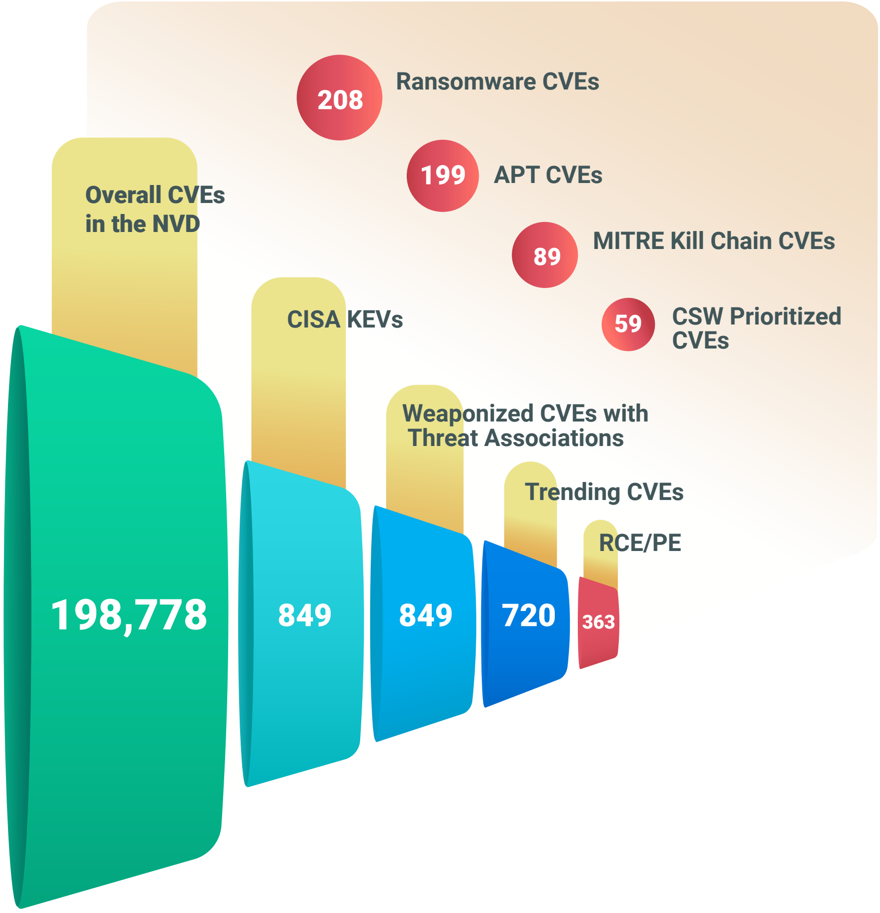
Key Observations

- All vulnerabilities in CISA KEV were observed to be weaponized, with 42% of them categorized as dangerous Remote Code Execution (RCE) and Privilege Escalation (PE) exploits.
- 52% of KEVs have publicly known exploits which justifies their inclusion in the catalog.
- We observed that 84% of vulnerabilities in the KEV catalog are trending[1] right now which reaffirms CISA's strict deadlines.
- We observed 24% of KEVs are being exploited by ransomware groups and 23% of them by threat groups which explains the core reason for CISA's KEV directive.
- 89 CVEs have a complete ATT&CK kill chain which can aid attackers from Infiltration to complete takeover of systems. These CVEs are extremely dangerous and need to be patched immediately.
- Microsoft, Apple, Google, CISCO, and Adobe are the top five vendors whose products have the maximum KEvs. Interestingly, 34% of KEVs exist in Microsoft products.
  Microsoft Windows 10 product has the maximum number of KEVs with 129 vulnerabilities.

[1] These are vulnerabilities that are actively being used in-the-wild.

CISA KEV Metrics & Threat Associations

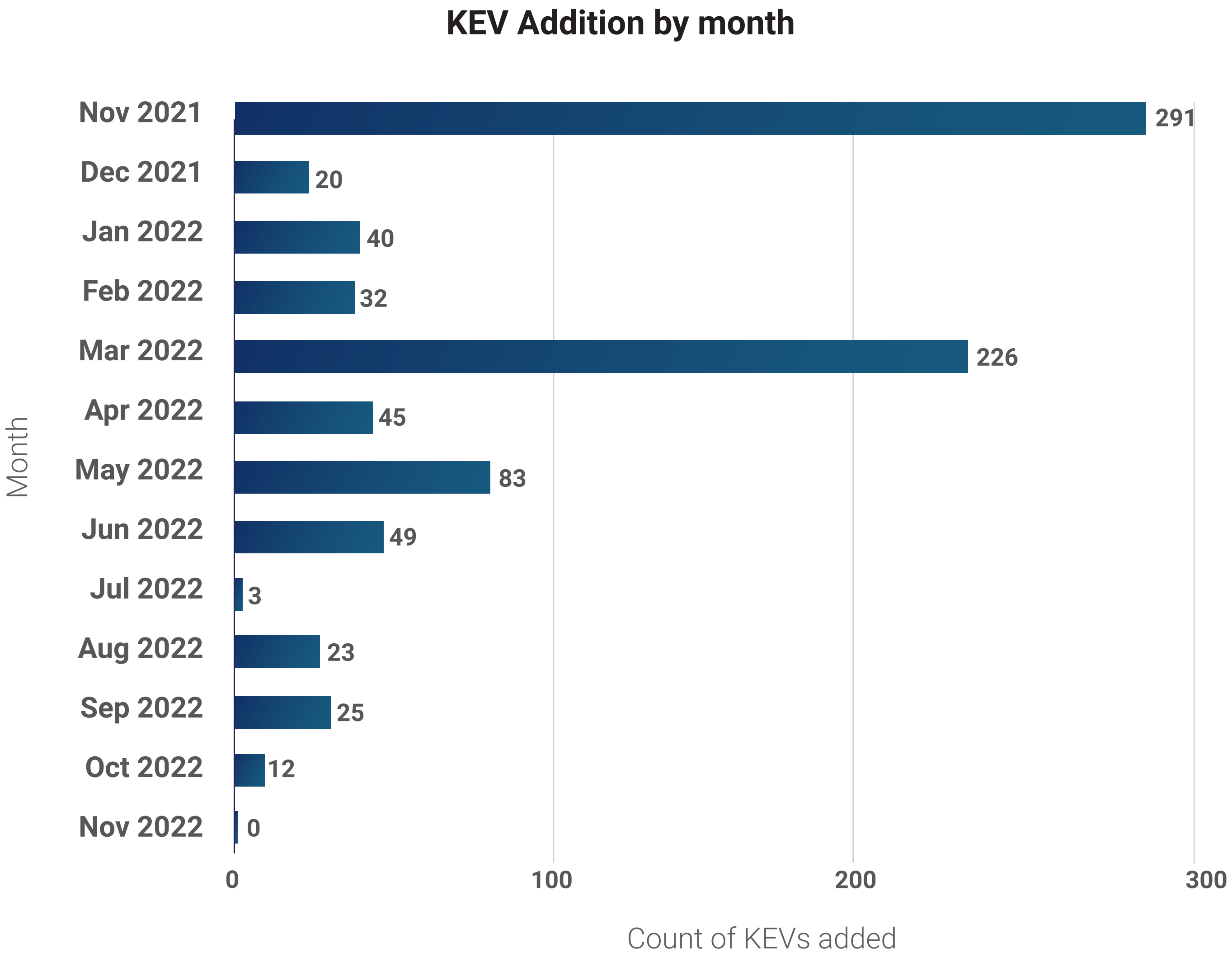
CSW's experts have been analyzing these vulnerabilities for a year, and here is how we have categorized this catalog based on threat associations and prioritization.



As evident, 42% of CISA's KEVs belong to the most dangerous exploit types, such as Remote Code Execution (RCE) and Privilege Execution (PE), 36% of them are associated with either associated ransomware or Advanced Persistent Threat (APT) groups, and 12% of them with both. Our researchers also observed that 84% of the vulnerabilities in the KEV Catalog are trending right now in the deep and dark web and hacker chats, validating the efforts that CISA is making.

Criteria for CISA’s KEVs

CISA has no fixed date to update the KEV Catalog, and no fixed number of vulnerabilities is added to the KEV every month. Sometimes, over 100+ vulnerabilities are added en masse; other times, even a single vulnerability is added to the catalog.



This shows that the minute a vulnerability matches the criteria to become a KEV, CISA wastes no time in updating the list.

A spike in the number of KEVs added can be seen in March 2022, when 226 vulnerabilities were added. This happened because CISA changed important criteria for adding vulnerabilities to the KEV Catalog. CISA started including vulnerabilities that were exploited in the past, irrespective of whether they are trending now. In this update, vulnerabilities discovered almost 20 years ago (from 2002 onward) were added to the KEV Catalog in March 2022.

There are 10,601 weaponized vulnerabilities,[2] which are about 6.8% of overall vulnerabilities (154,790) considered for the research. Yet, CISA has added only 849 weaponized vulnerabilities in its KEV Catalog. This is because vulnerabilities in the KEV Catalog are selected based on the following three criteria:

- **Assigned CVE ID:** The first criterion is that the vulnerability should have a CVE ID (also known as the CVE identifier).
- **Active Exploitation:** The second criterion examines if a vulnerability is exploitable, [3] has already been exploited, or is under active exploitation. CISA describes this criterion as vulnerabilities for which reliable evidence is available that a malicious code was executed by an attacker on a system.
- **Clear Remediation Guidance:** The third criterion looks at the remediation guidance for a vulnerability and selects those for which an official patch or a workaround is available. This criterion makes the KEV Catalog actionable, enabling public sector organizations to take action against these vulnerabilities and become resilient.

Here are a few examples of vulnerabilities that are trending threats but are not a part of CISA KEVs yet. However, these vulnerabilities do not fit into the KEV criteria, owing to factors like missing patches or the lack of evidence of active exploitation. Nonetheless, we are noticing higher interest in these threats in hacker channels and urge users to be extra vigilant in tracking vendor updates for these vulnerabilities.

Trending Non-KEV That Deserve Attention

Vulnerability	Vendor	Product	CVSS (v3) Severity
CVE-2021-24284	Kaswara Project	Kaswara	Critical
CVE-2020-26879	CommScope	Ruckus Vriot	Critical
CVE-2020-26878	CommScope	Ruckus Vriot	High
CVE-2020-12501	Pepperl+Fuchs, Korenix	Multiple firmware versions	Critical
CVE-2018-6055	Google	Chrome	High
CVE-2022-3180	WordPress	WPGateway	-

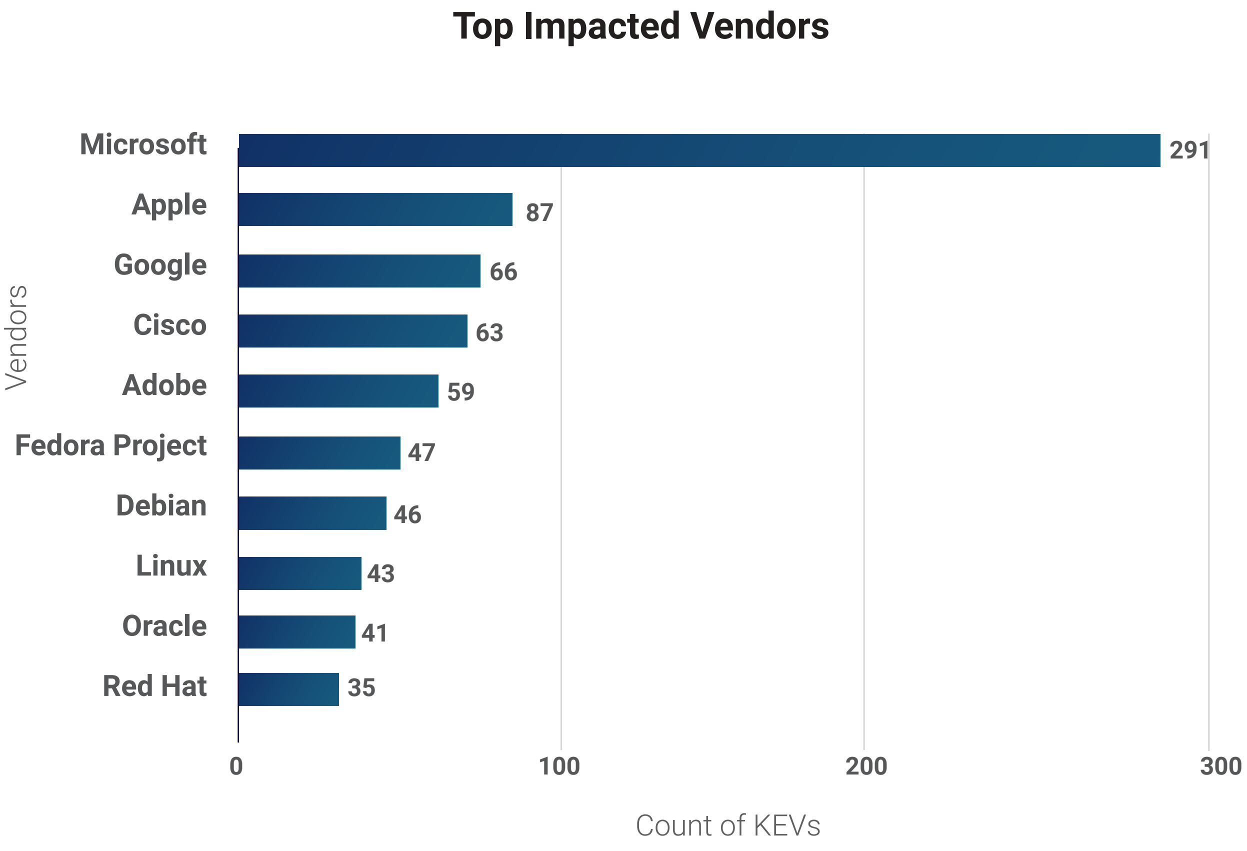
[2] As per our Ransomware Report released on Oct. 20, 2022

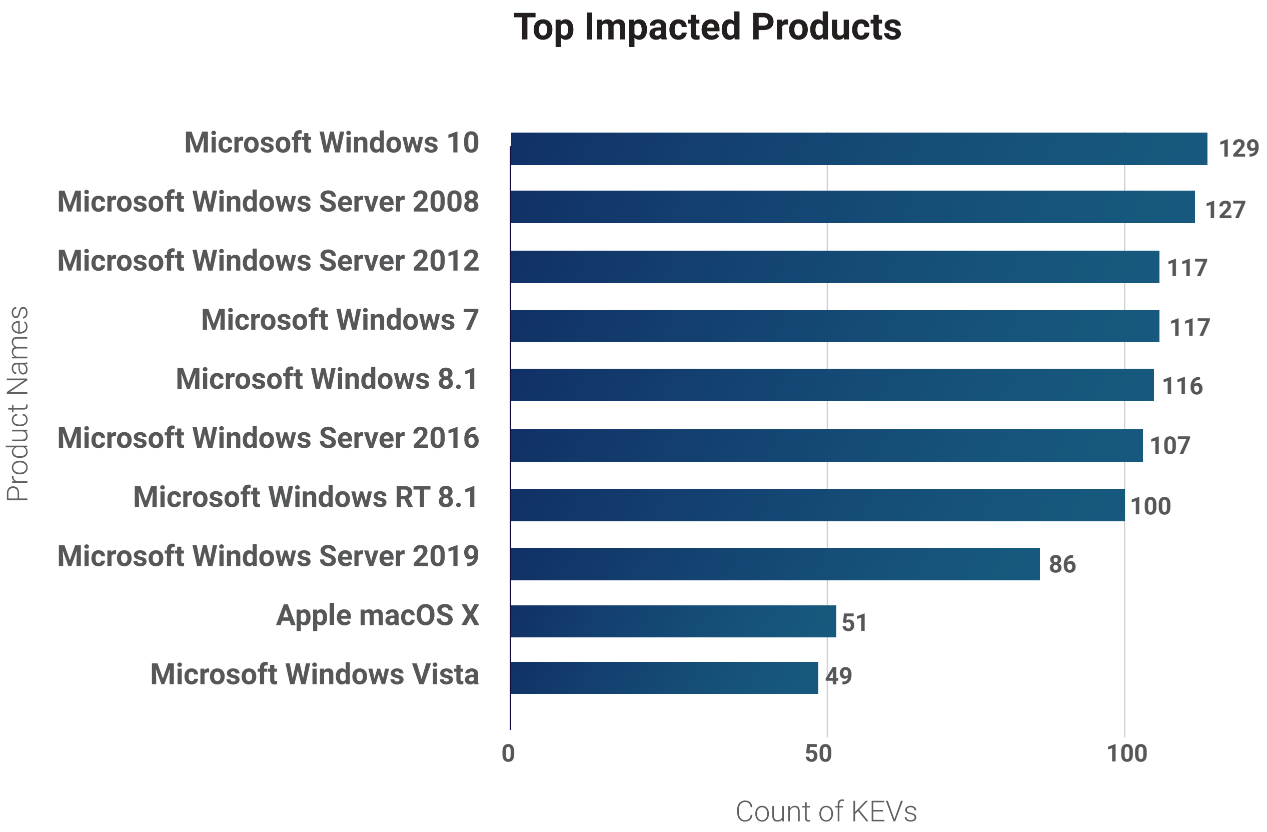
[3] The term "exploitable" refers to how easily an attacker can take advantage of a vulnerability.

Impacted Vendors and Products

When we examined the vendors and products featured in the CISA KEV Catalog, we found Microsoft, Apple, Google, CISCO, and Adobe in the top five. Interestingly, vulnerabilities in Microsoft's products cover 34% of CISA's KEV Catalog, with one out of three KEVs impacting products from this vendor.

With over 181 unique vendors and 3,084 unique products, the KEV Catalog is littered with vulnerabilities affecting key product segments such as remote services and applications (VPNs and firewalls), network devices (routers and switches), web application frameworks (content management software, web applications, and HTTP servers), and information repositories. We have also observed backup storage services affected by at least 4% of these vulnerabilities.





Among the most impacted products, Microsoft Windows 10 is leading with the maximum number of KEVs. Some interesting callouts would be Microsoft Internet Explorer, Adobe Flash Player, Windows Vista, Windows Server 2003, Windows 8, Windows XP, Windows 2003 Server, CISCO RV340 Firmware, Windows 2000, and Silverlight; these are products that have reached the end of life (EOL)—meaning the vendor has decided to discontinue these products, necessitating the need for its users to upgrade to the next version of the product.

Products such as Windows Server 2008 and Windows 7 are classified as the end of service life (EOSL) when the vendor stops providing support or updates for the said software. Interestingly, Windows Server 2008 has 127 KEVs, and Windows 7 has 117 KEVs, highlighting that attackers are targeting these products to take advantage of the lack of support and updates.

Unsurprisingly, organizations that continue to use EOL and EOSL products become easy targets for attackers.

Exploit Analysis

Since weaponization is one of the most important criteria for addition to CISA's KEV Catalog, we consider all vulnerabilities in the KEV as weaponized, and 52% of them have publicly known exploits.

When our researchers examined the exploit count, we found that CVE-2017-11882, a Microsoft Office vulnerability, had no less than 1,476[4] exploits available in the public domain. Interestingly, the CVSS V2 score for this vulnerability is 9.3 (high), and the CVSS V3 score is 7.8 (high).

Other CVEs with a high number of exploits are Microsoft vulnerabilities CVE-2017-0199, CVE-2017-8570, and CVE-2022-30190, with 648[5], 146, and 41 publicly known exploits, respectively.

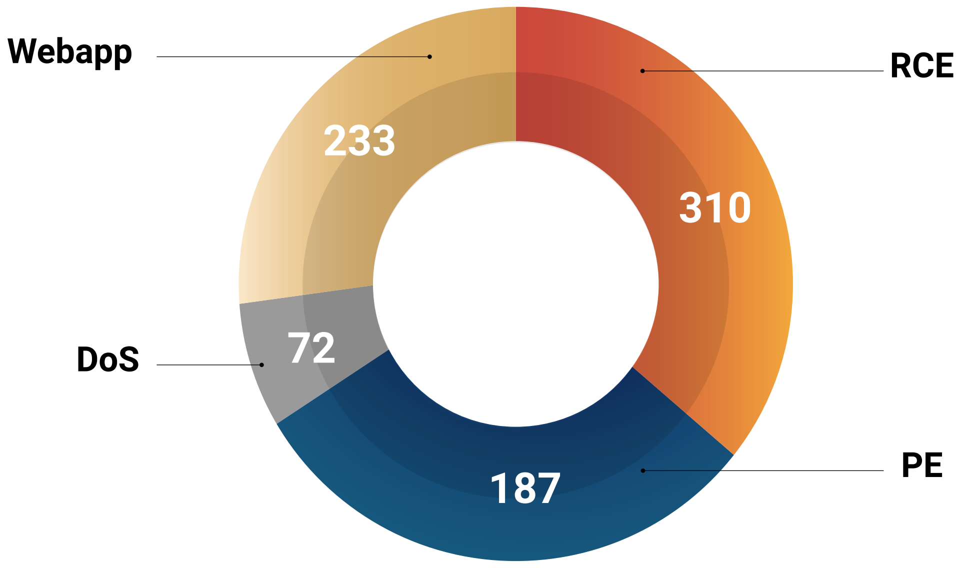
CVE-2017-11882
Microsoft Office

CVSS V2 : 9.3 (High)
CVSS V3 : 7.8 (High)
Securin VRS : 9.24 (Critical)

1,476
Publicly Available
Exploits

Next, we examined the type of exploits to which KEVs belong and found 36% of the vulnerabilities belong to Remote Code Execution (RCE) and 22% belong to Privilege Execution (PE). CSW's experts consider RCE and PE exploit types extremely dangerous and should be prioritized for patching.

Exploit Type—Distribution

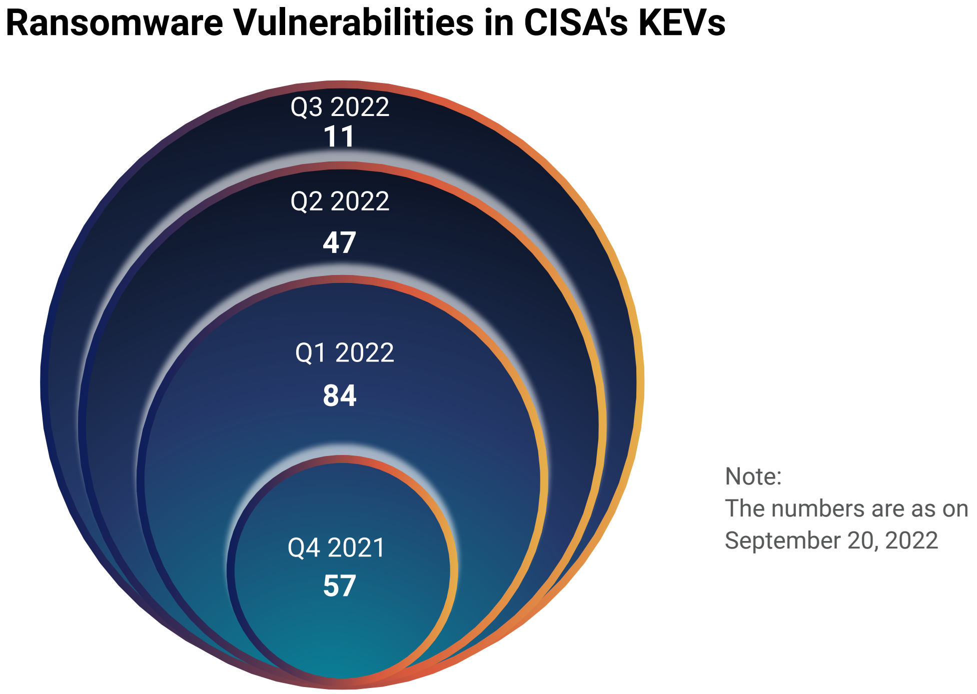


[4,5] The count includes all distinct variants of the exploit

Threat Associations

An important thing missing in the present KEV Catalog is the threat association for each vulnerability. While CISA is mandating the FCEB agencies to patch the KEVs from the catalog, it does not provide any information as to why a vulnerability needs to be patched. CSW's researchers fill this gap using our ransomware database and have found that 36% of the KEVs are associated with either Ransomware or APT groups.

CSW's experts have been tracking ransomware vulnerabilities and their exploitation by numerous ransomware operators since 2019. In our last quarter report published on October 20, 2022, we were able to confirm that a total of 323 vulnerabilities are now being exploited to mount ransomware attacks.


Ransomware Vulnerabilities in CISA's KEVs

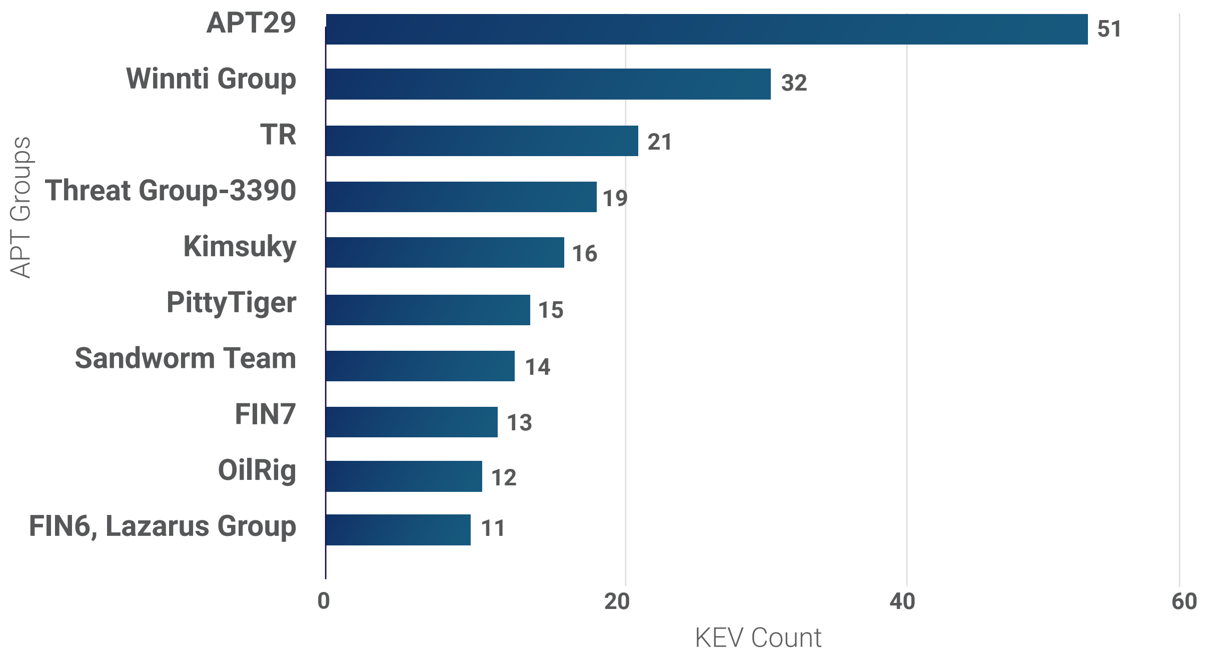
Note:
The numbers are as on
September 20, 2022

A Screenshot from the Ransomware Report Q2-Q3 2022 Published on October 20, 2022

We found that 208 vulnerabilities in CISA's KEV Catalog are associated with ransomware (as of November 03, 2022), and 199 of them are being used by APT groups. We also observed that 104 vulnerabilities are being used by both ransomware and APT groups.

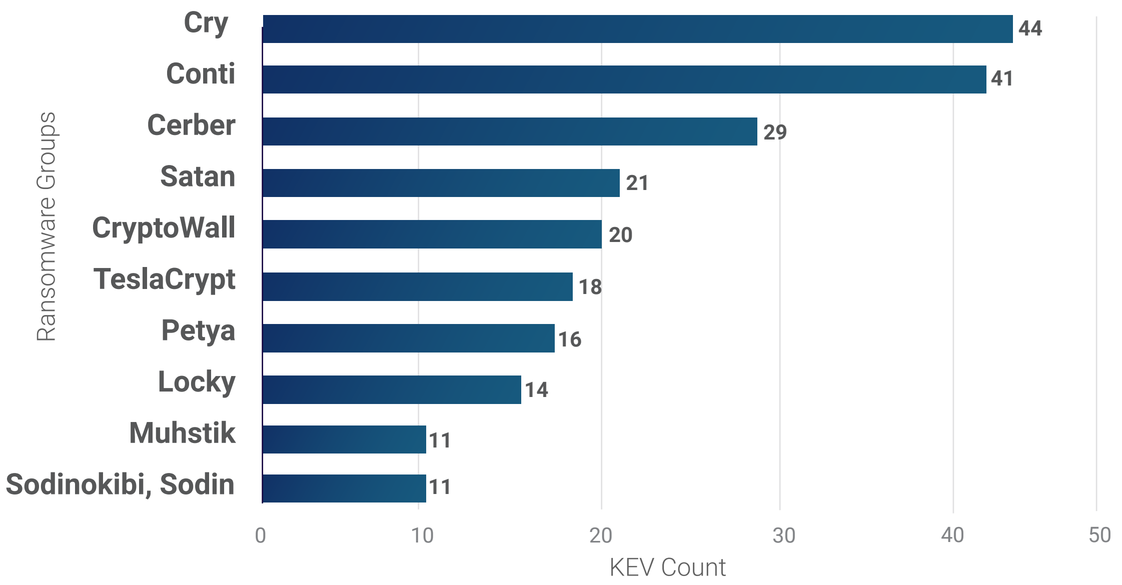
Of the 208 ransomware vulnerabilities, many are being exploited by multiple ransomware groups. For example, CVE-2013-3896, a Microsoft medium severity vulnerability, has no less than 39 ransomware associations! Microsoft vulnerabilities CVE-2012-0158 and CVE-2017-11882 have been rated critical and high, respectively, and are being exploited by 23 APT groups. As recently as November 2022, these vulnerabilities have been exploited by the Thrip APT group, also called Lotus Blossom/BitterBug, in their campaigns.

Top APT Groups with KEVs



APT 29, also known as the Nobelium group, stands at the top of the list exploiting 51 KEVs. State-sponsored by Russia, this threat group is behind the infamous SolarWinds supply chain attack in December 2021.

Top Ransomware Groups with KEVs



Among the ransomware groups, Cry is at the top of the list exploiting 44 vulnerabilities, followed by Conti and Cerber.

Here is a list of the top vulnerabilities present in the KEV Catalog with the maximum ransomware and threat group associations:

Top 5 Vulnerabilities with Ransomware Associations

CVE ID	Vendor & Product	CVSS Severity	VRS Severity	Ransomware Association count
CVE-2013-3896	Microsoft Silverlight	Medium	High	39
CVE-2013-7331	Microsoft Internet Explorer	Medium	High	37
CVE-2017-0145	Microsoft SMBv1	High	Critical	20
CVE-2017-0144	Microsoft SMBv1	High	Critical	19
CVE-2017-0147	Microsoft SMBv1 server	Medium	High	15

Top Vulnerabilities with the Maximum APT Group Associations

CVE ID	Vendor & Product	CVSS Severity	VRS Severity	APT Association count
CVE-2012-0158	Microsoft MSCOMCTL.OCX	Critical	Critical	23
CVE-2017-11882	Microsoft MSCOMCTL.OCX	High	Critical	
CVE-2017-0199	Microsoft Windows, Windows Server, Office	High	Critical	17
CVE-2018-0802	Microsoft Office	High	High	14
CVE-2021-26855	Microsoft Exchange Server	Critical	Critical	
CVE-2021-27065	Microsoft Exchange Server	High	Critical	13
CVE-2021-26857	Microsoft Exchange Server	High	High	11
CVE-2021-26858	Microsoft Exchange Server	High	High	

In the Q3 Ransomware report, we found 57 vulnerabilities with a complete ATT&CK kill chain enabling attackers to completely take over the system from end to end, execute any code, freely move within the network, and manipulate and extract data. We observed that 48 out of 57 vulnerabilities had been included in the CISA KEV catalog justifying the need to patch these vulnerabilities at the earliest. An overall of 89 KEVs has a complete MITRE ATT&CK kill chain all the way from infiltrating a network to data exfiltration or malware execution, making their way easily through the network without detection.

With 323 ransomware vulnerabilities currently being exploited by attackers, we also noted that 124 of these (as of Q3 2022) are yet to be included in the CISA KEV Catalog. We highly recommend that these vulnerabilities be included in the KEV catalog as any vulnerability tied to ransomware or a threat group is tainted for life and needs to be prioritized for patching and remediation.

Conclusion

The Known Exploited Vulnerabilities Catalog is a valuable initiative undertaken by CISA. It provides an actionable list of vulnerabilities to FCEB agencies, mandating them with a directive to reduce the risk of cyberattacks to the nation's infrastructure.

While the binding directive applies only to the FCEB, CISA recommends that other organizations too use the KEV Catalog as an authoritative list to remediate vulnerabilities that are sought out by attackers.

Through this report, CSW's experts have filled in the threat context that is missing in the KEVs; through our analysis, we have also highlighted why CISA felt the need to launch this initiative.

CSW's experts will continue our vulnerability research, provide federal and public sector companies with more insights about the KEVs and help them meet their remediation deadlines.

> **“Over the past year CISA has identified and shared more 849 and counting Known Exploitable Vulnerabilities. Our mission is to provide early warning security intelligence to all our customers. We are providing critical insights to our customers on most vulnerabilties more than 20 days prior to CISA adding it to their list! We will continue to innovate and help our customers improve their security posture!**
>
> **Aaron Sandeen, CEO & Co-founder, CSW & Securin**

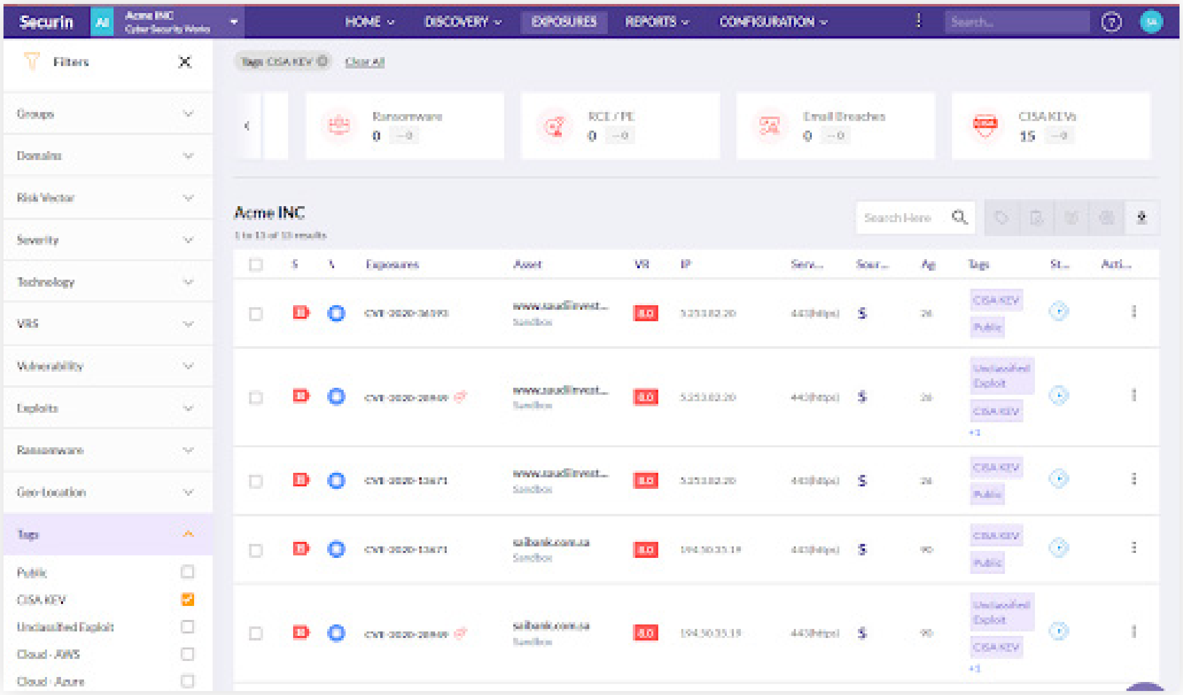
How Is CSW Helping Federal Entities and Public Sector Companies?

Right from the time CISA launched the KEV catalog, CSW's experts have analyzed and highlighted the threat context associated with this repository. Here is how we are using this repository to help our customers.

Securin's Attack Surface Management (ASM)

Securin's Attack Surface Management solution helps organizations discover, analyze, prioritize, and mitigate vulnerabilities and exposures that would attract attackers to breach their enterprise. Securin's ASM provides a hacker's view of the attack surface, giving our customers a holistic view of their cyber hygiene. We provide our customers with a dynamic filtered view of the CISA KEVs in their attack surface, expediting remediation and mitigation.

Securin's ASM with CISA's KEV Filter



Public ☐
CISA KEV ☑
Unclassified Exploit ☐
Cloud - AWS ☐
Cloud - Azure ☐

Ransomware 0 — 0
RCE / PE 0 — 0
Email Breaches 0 — 0
CISA KEVs 15 — 0

Acme INC

1 to 13 of 13 results

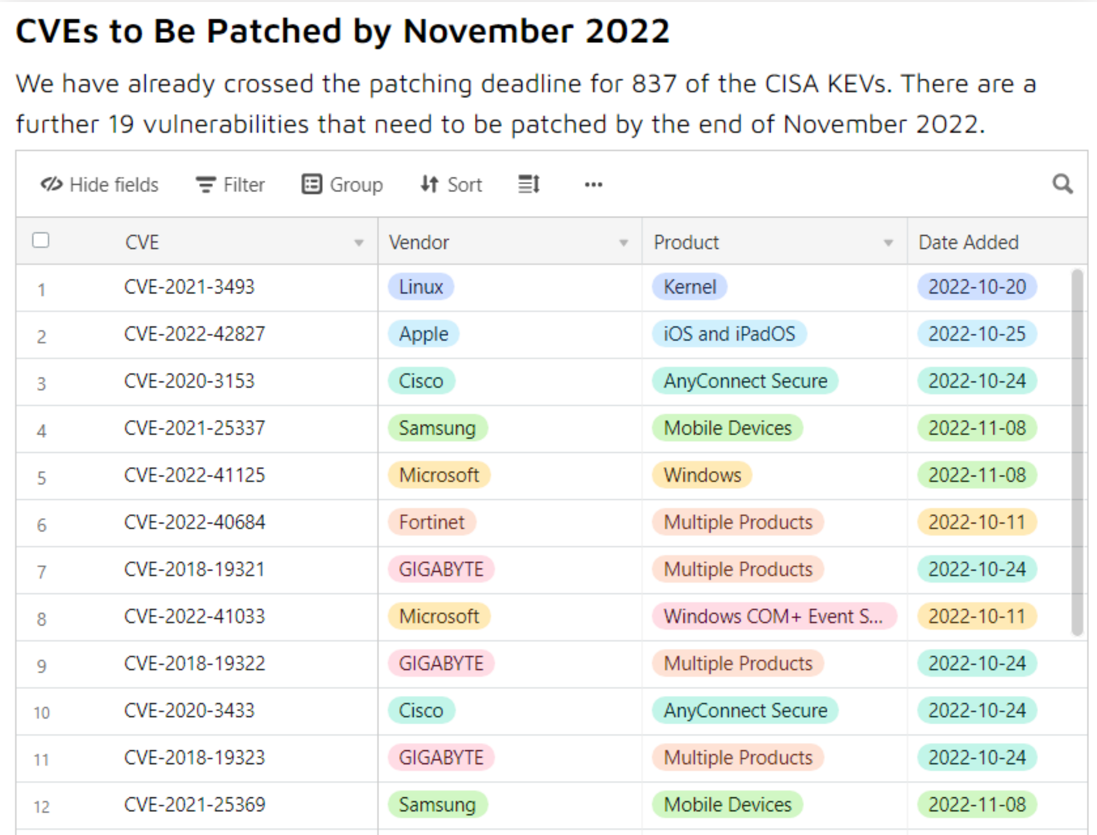
☐	S	\	Exposures	Asset	VR	IP	Serv...	Sour...	Ag	Tags	St...	Acti...
☐			CVE-2020-36193	www.saudiinvest... Sandbox	8.0	5.253.82.20	443(https)	$	26	CISA KEV Public		⋮
☐			CVE-2020-28949	www.saudiinvest... Sandbox	8.0	5.253.82.20	443(https)	$	26	Unclassified Exploit CISA KEV +1		⋮
☐			CVE-2020-13671	www.saudiinvest... Sandbox	8.0	5.253.82.20	443(https)	$	26	CISA KEV Public		⋮
☐			CVE-2020-13671	saibank.com.sa Sandbox	8.0	194.50.35.19	443(https)	$	90	CISA KEV Public		⋮
☐			CVE-2020-28949	saibank.com.sa Sandbox	8.0	194.50.35.19	443(https)	$	90	Unclassified Exploit CISA KEV +1		⋮

Vulnerability Management

Our experts continuously scan our customers' networks for vulnerabilities and alert them whenever CISA adds new vulnerabilities to the KEV Catalog. We provide additional threat context to these KEVs and prioritize them for our customers to patch immediately.

CISA's KEVs—Exclusive Blog and Patches

CSW continuously updates an exclusive blog on CISA's KEVs, where we discuss the threat context at length and provide bite-sized information for our customers and readers to consume.



CVEs to Be Patched by November 2022

We have already crossed the patching deadline for 837 of the CISA KEVs. There are a further 19 vulnerabilities that need to be patched by the end of November 2022.

□	CVE	Vendor	Product	Date Added
1	CVE-2021-3493	Linux	Kernel	2022-10-20
2	CVE-2022-42827	Apple	iOS and iPadOS	2022-10-25
3	CVE-2020-3153	Cisco	AnyConnect Secure	2022-10-24
4	CVE-2021-25337	Samsung	Mobile Devices	2022-11-08
5	CVE-2022-41125	Microsoft	Windows	2022-11-08
6	CVE-2022-40684	Fortinet	Multiple Products	2022-10-11
7	CVE-2018-19321	GIGABYTE	Multiple Products	2022-10-24
8	CVE-2022-41033	Microsoft	Windows COM+ Event S...	2022-10-11
9	CVE-2018-19322	GIGABYTE	Multiple Products	2022-10-24
10	CVE-2020-3433	Cisco	AnyConnect Secure	2022-10-24
11	CVE-2018-19323	GIGABYTE	Multiple Products	2022-10-24
12	CVE-2021-25369	Samsung	Mobile Devices	2022-11-08

Over the past year CISA has identified and shared more 849 and counting Known Exploitable Vulnerabilities. Our mission is to provide early warning security intelligence to all our customers. We are providing critical insights to our customers on most vulnerabilties more than 20 days prior to CISA adding it to their list! We will continue to innovate and help our customers improve their security posture!

CSW's experts can help you remediate CISA's KEVs using our solutions and services.

Talk To Us

About CSW

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.

CSW Cyber SecurityWorks

About Securin

Securin helps customers gain resilience against evolving threats. Powered by accurate vulnerability intelligence, human expertise, and automation, Securin's products and services have enabled organizations to make critical security decisions in managing their attack surface.

For more information, visit www.securin.io.

Securin