The VulnCheck 2022 Exploited Vulnerability Report - Missing CISA KEV Catalog Entries

vulncheck.com/blog/2022-missing-kev-report

Go back

March 9, 2023

Jacob Baines

The data in this report was generated on March 2, 2023. Any additions to the CISA KEV Catalog after that date are not reflected in this report.

In last week's blog, we looked at the vulnerabilities the Cyber Security & Infrastructure Agency (CISA) added to the Known Exploited Vulnerability (KEV) Catalog in 2022. In the report,we mentioned CISA missed some actively exploited vulnerabilities that had been assigned CVEs in 2022. The KEV Catalog is the driving force for vulnerability management in the US federal civilian executive branch, and many private companies have adopted it as

the de facto standard. As such, excluding any exploited-in-the-wild vulnerability is a big deal with potentially far-reaching effects. This blog will share 42 likely exploited-in-the-wild vulnerabilities assigned CVEs in 2022 that haven't been included in the KEV Catalog.

Key Takeaways

- VulnCheck identified 42 vulnerabilities that were assigned CVEs in 2022 and reported to have been, or likely to have been, exploited in the wild that were not added to the CISA KEV Catalog.
- Of the 42 CVEs, an overwhelming majority are related to botnets (64%). However, there are also a number of ransomware (10%) and threat actor (12%) attributions.
- Some missing vulnerabilities, specifically CVE-2016-20016, have been exploited in the wild since 2017 and still have thousands of potential targets online.
- 76.2% of the missing vulnerabilities were initial access, which VulnCheck recommends prioritizing.
- The CISA KEV Catalog is undoubtedly helpful and a driving force in our industry. Still, as long as it's missing actively exploited vulnerabilities, it cannot be treated as the authoritative catalog of exploited vulnerabilities.

The Missing Vulnerabilities

Using publicly-available reporting, VulnCheck identified 42 vulnerabilities that were assigned CVEs in 2022 and reported to have been, or likely to have been, exploited in the wild. The exploited-in-the-wild sources include a variety of world-class security organizations, including Talos, ESET Research, Avast, FortiGuard Labs, Rapid7, and more.

The public reporting often tells us *who* was doing the exploitation: ransomware, botnets, threat actors, etc. The "who" is essential, as it can change the criticality of a vulnerability. A vulnerability exploited by ransomware is much more concerning than a vulnerability exploited by a Mirai botnet. VulnCheck breaks down the "who" into four general "attacker-type" categories:

1. Botnets (e.g. Mirai, Zerobot, etc.)
2. Ransomware (e.g Clop)
3. Threat Actors (e.g. APT32)
4. Unattributed (a source notes exploitation in the wild but doesn't provide any attribution information)

The following table contains all 42 vulnerabilities, the reported attacker type, and the publicly-available source indicating likely exploitation in the wild.

CVE-ID	VulnCheck Attacker-Type	Exploited Source

CVE-ID	VulnCheck Attacker-Type	Exploited Source
CVE-2022-45359	Unattributed	Wordfence
CVE-2022-45045	Botnet	VulnCheck, 360 Netlab
CVE-2022-39197	Threat Actor	360
CVE-2022-37061	Botnet	FortiGuard Labs, 360 Netlab
CVE-2022-35914	Unattributed	FR-CERT, Unit 42
CVE-2022-35526	Botnet	FortiGuard Labs (see Unknown 2)
CVE-2022-34721	Threat Actor	CYFIRMA
CVE-2022-34538	Botnet	FortiGuard Labs, 360 Netlab
CVE-2022-31499	Unattributed	Unit 42
CVE-2022-31199	Ransomware	Talos
CVE-2022-28810	Threat Actor	ESET Research, Rapid7
CVE-2022-27510	Ransomware	At-Bay
CVE-2022-27226	Botnet	FortiGuard Labs
CVE-2022-26809	Ransomware	Group-IB
CVE-2022-26504	Ransomware	Cloudsek
CVE-2022-26210	Botnet	FortiGuard Labs, Unit 42
CVE-2022-26186	Botnet	FortiGuard Labs, Unit 42
CVE-2022-25084	Botnet	FortiGuard Labs
CVE-2022-25083	Botnet	FortiGuard Labs
CVE-2022-25082	Botnet	FortiGuard Labs
CVE-2022-25081	Botnet	FortiGuard Labs
CVE-2022-25080	Botnet	FortiGuard Labs
CVE-2022-25079	Botnet	FortiGuard Labs
CVE-2022-25078	Botnet	FortiGuard Labs
CVE-2022-25077	Botnet	FortiGuard Labs
CVE-2022-25076	Botnet	FortiGuard Labs

CVE-ID	VulnCheck Attacker-Type	Exploited Source
CVE-2022-25075	Botnet	FortiGuard Labs, Alien Labs, Unit 42
CVE-2022-24934	Threat Actor	Avast
CVE-2022-2486	Unattributed	Threat Actor
CVE-2022-24500	Ransomware	Group-IB
CVE-2022-23714	Ransomware	Group-IB
CVE-2022-2003	Botnet	Dragos
CVE-2022-0456	Threat Actor	Group-IB
CVE-2021-46850	Botnet	Talos (see VestaCP)
CVE-2021-46422	Botnet	FortiGuard Labs, 360 Netlab
CVE-2021-41506	Botnet	Trend Micro
CVE-2021-4045	Botnet	FortiGuard Labs
CVE-2021-4039	Botnet	Alien Labs
CVE-2021-31805	Botnet	360 Netlab
CVE-2017-20149	Botnet	360 Netlab, NDSS Symposium
CVE-2016-20017	Botnet	360 Netlab, ESET Research
CVE-2016-20016	Botnet	Trend Micro, ESET Research

Botnets

Looking over the table, it's probably obvious that an overwhelming majority of the vulnerabilities are related to botnets (64%). However, there are also a number of ransomware (10%) and threat actor (12%) attributions.

> Attacker-Type of Exploited Vulnerabilities Assigned CVE in 2022 Missing From CISA KEV

The high rate of botnet-exploited vulnerabilities is interesting. Mirai-like botnets are well-known for flinging exploits all over the internet. That behavior is quickly picked up by honeypots and intelligence-sharing organizations like Unit 42, 360 Netlab, and Fortiguard Labs. The high volume of botnet vulnerabilities should be some of the easiest to classify as exploited in the wild.

For example, one of the 42 vulnerabilities missing from the CISA KEV Catalog is CVE-2016-20016 (aka EDB-41471). This vulnerability, which finally received a CVE in 2022, has been exploited in the wild for years, and still has thousands of potential targets online. It's had a Metasploit module since 2017 and is routinely one of the most widely attempted exploit targets on both ShadowServer and Greynoise. The NVD entry even notes "exploited in the wild in 2017 through 2022." It's obvious this vulnerability belongs in the KEV Catalog.

Vulnerability Classification and Exploits

Last week, we analyzed the type of vulnerabilities that were added to KEV in 2022. We found about ⅓ of the vulnerabilities are Initial Access, ⅓ are Client Side, and the other ⅓ fell to the remaining five vulnerability types that VulnCheck assigns. However, the 42 missing vulnerabilities don't match that pattern,likely due to the healthy helping of botnet-exploited vulnerabilities.

> Missing Exploited Vulnerabilities Classification

At VulnCheck, we're very interested in initial access vulnerabilities specifically because they are so dangerous. Many of these vulnerabilities appear to provide initial access to small routers and IoT systems. Some will dismiss vulnerabilities in such targets. However, we know those types of targets are used by advanced threat actors to create massive botnets like VPNFilter, and(taken down just last year) Cyclops Blink. So, these vulnerabilities should be taken seriously.

They should also be taken seriously because most of them are well-known. More than 30 of the vulnerabilities have public exploits, and at least four of those have Metasploit modules. Additionally, seven have commercially available exploits.

> Exploited Vulnerabilities with Exploits

Individual Vulnerabilities

Each of the missing 42 vulnerabilities have interesting context around them too, partly due to the many different sources and unique points of view shared in their public reporting. Going through each would be tedious, but the following sections give insight into a few vulnerabilities that should give readers a general feel for the top vulnerabilities CISA missed.

Chimay Red

CVE-2017-20149, also known as Chimay Red, is a peculiar case. The details of the vulnerability were originally leaked in 2017 during the Vault 7 leak. The vulnerability affected the HTTP interface of Mikrotik routers (of which, there are currently more than 600k visible

on Shodan). Shortly after the disclosure, a high quality exploit was developed by Lorenzo Santina. Eventually attackers, including the Hajime botnet, exploited this vulnerability in the wild.

While the vulnerability is getting old, Greynoise continues to see active scanning for the vulnerability and, using Shodan, we can find approximately 10,000 internet-facing hosts that are still vulnerable.

However, the most fascinating part of Chimay Redis that it didn't receive a CVE until 2022 when VulnCheck requested one (MITRE chose to back-date the year). This vulnerability has been exploited in the wild for approximately five years, and no one saw fit to request a CVE. Having a CVE *is a requirement to be included in the CISA KEV Catalog*, and, sadly, appears to be the only way to remain in the vulnerability historical record.

It's also worth noting that back when the Shadow Brokers leak occurred, there was an effort to identify and assign CVE to zero-day vulnerabilities that had been leaked. This was obviously not the case here. The responsible parties should have done the right thing and ensured this was assigned a CVE five years ago. Maybe there wouldn't be any more vulnerable internet-facing Mikrotik routers if they did.

CVE-2022-28810

CVE-2022-28810 is an authenticated unrestricted operating system command execution vulnerability affecting ManageEngine ADSelfService Plus. ManageEngine products have been included in several CISA advisories. For example, in October 2022, a ManageEngine vulnerability, CVE-2021-40539, was included in a bulletin titled, *Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors*.

This vulnerability was first seen in the wild in April 2022 as a zero-day by Rapid7 (full disclosure: this author was involved in the analysis of the vulnerability). Additionally, ESET Research noted in their APT Activity Report T2 2022 report that a "defense contractor in the US" was targeted using this vulnerability. Although ESET couldn't attribute the attack to a specific group, it was lumped in with "China-aligned" APT activity.

CVE-2022-2003

Dragos researchers shared a great writeup on finding CVE-2022-2003 in the wild. The vulnerability was discovered in a PLC "password cracking" program advertised on social media. Dragos found the cracking software actually worked as advertised, and the software recovered passwords from AutomationDirect's DirectLOGIC PLC by exploiting CVE-2022-2003. Also, hilariously, the cracking software drops malware on the host machine in order to join it to the Sality botnet.

ICS-specific vulnerabilities exploited in the wild are few and far between. Dragos uncovered an attacker specifically targeting PLC and engineering workstations. Given the attacker's active engagement on social media, this vulnerability seems like it should have been an easy add to the KEV Catalog.

CVE-2022-31199

Cisco Talos was able to link CVE-2022-31199, a vulnerability in Netwrix Auditor, to Truebot activity (and eventually Clop ransomware) in an early December 2022 blog.

An advisory for CVE-2022-31199 was published by Bishop Fox in July 2022. The advisory has no CVE, but it is linked directly to NVD. To our knowledge, there is no public exploit for this vulnerability. However, the Bishop Fox advisory, from our experience, provides sufficient details to recreate the exploit with minimal effort. That's likely why Talos saw the vulnerability exploited a "few weeks" after the advisory was published.

Netwrix Auditor isn't exactly a household name, and there are fewer than a dozen internet-facing targets. The fact that an attacker chose to weaponize this vulnerability and it was exploited in the wild shows how valuable initial access vulnerabilities are to attackers.

Conclusion

In this blog, we shared 42 vulnerabilities assigned CVEs in 2022, which were publicly reported to be exploited in the wild. Yet, none of these vulnerabilities are in the CISA KEV Catalog. The CISA KEV Catalog is undoubtedly helpful and a driving force in our industry. Still, as long as it's missing actively exploited vulnerabilities, it cannot be treated as the authoritative catalog of exploited vulnerabilities. Practitioners should augment vulnerability management programs by seeking out additional sources or finding a source with a more complete dataset.

For more information on vulnerabilities exploited in the wild, register for a VulnCheck account today by loading https://vulncheck.com and clicking "Log In".