**CISA's Known Exploited Vulnerabilities Catalog – March 2022 Archive**

*March 31, 2022*

*Note: this was updated from 8 to 7 on 4/1/2022 to reflect 1 removal by CISA as it was a duplicate that had been previously added on 3/25/2022.*

On **March 31, 2022**, CISA added **7** new vulnerabilities to its Known Exploited Vulnerabilities Catalog. All 7 additions are for CVE's from 2018 – 2022 across **6** products that threat actors are currently using to exploit systems that remain unpatched. The new vulnerabilities have a remediation/address by due date of 4/21/2022.

CISA's Known Exploited Vulnerabilities Catalog is a highly recommended resource to help all organizations prioritize patching in (mostly) IT environments. Likewise, the remediation due dates offer granularity in approaching and understanding the importance of patch prioritization. While the due dates are intended for federal agency networks, as always it is recommended that all organizations follow suit to best protect their environments from publicly exploited vulnerabilities.

Members are encouraged to check the catalog and the regular updates for potentially impacted components in your environment.

The 7 newly added vulnerabilities impact the following 6 products/vendors/platforms:

- Dasan (2)
- Dell
- Microsoft
- QNAP
- Sophos
- Trend Micro

The **full catalog** (downloadable in various formats) can be accessed here: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

*March 29, 2022*

On **March 25, 2022**, and **March 28, 2022**, CISA added **66** and **32** new vulnerabilities, respectively, to its Known Exploited Vulnerabilities Catalog. All **98** additions are for CVE's from 2015 – 2020 across **38** products that threat actors are currently using to exploit systems that remain unpatched. The new vulnerabilities have a remediation/address by due dates of 4/15/2022 and 4/18/2022, respectively.

The newly added vulnerabilities impact the following **38** products/vendors/platforms:

- Adobe (7)
- Apache (4)
- Arcserve
- Atlassian
- Cisco (6)
- Citrix (4)
- D-Link (4)
- D-Link and TRENDnet
- Drupal
- Elastic (2)
- Exim (2)
- Google
- Hewlett Packard (HP) (2)
- Jenkins

- Juniper
- Kentico
- LG
- Microsoft (28)
- Mitel
- NETGEAR (3)
- OpenBSD
- Oracle (4)
- Palo Alto
- PHP (2)
- phpMyAdmin
- QNAP Systems
- Quest
- Rails (2)
- Redis
- Rejetto
- Sitecore
- SonicWall (2)
- Sophos
- TP-Link
- VMware (3)
- WatchGuard
- Webmin
- Zyxel

*March 17, 2022*
On March 15, 2022, CISA added **15** new vulnerabilities to its Known Exploited Vulnerabilities Catalog with CVE's from 2015 – 2020 that threat actors are currently using to exploit systems that remain unpatched. All added vulnerabilities have a remediation due date of 4/5/2022.

Members are encouraged to check the catalog and the regular updates for potentially impacted components in your environment.

The newly added vulnerabilities impact the following products/vendors/platforms:
- SonicWall
- Microsoft (14)

*March 8, 2022*
On March 7, 2022, CISA added **11** new vulnerabilities to its Known Exploited Vulnerabilities Catalog with CVE's from 2009 – 2022 that threat actors are currently using to exploit systems that remain unpatched. The Mozilla Firefox and VMware vCenter Server and Cloud Foundation vulnerabilities have a remediation due date of 3/21/2022.

Today's 11 is in addition to the 95 vulnerabilities added last week, which included the first industrial control product – Siemens SIMATIC CP 1543-1 (CVE-2016-8562 with an address by due date of 3/24/2022). In addition, last week's 95 vulnerabilities also included a 20 year old vulnerability for a couple of 20+ year old operating systems (Microsoft Windows NT and Windows 2000) – indicating threat actors are still attacking them because they are still finding them.

CISA's Known Exploited Vulnerabilities Catalog is a highly recommended resource to help all organizations prioritize patching in IT environments. Likewise, the remediation due dates offer even more granularity in approaching and understanding the importance of patch prioritization. While the due dates are intended for federal networks, as always it is recommended that all organizations follow suit to best protect their environments.

Members are encouraged check the catalog and the regular updates for potentially impacted components in your environment.

The newly added vulnerabilities impact the following products/vendors/platforms:

- Mozilla Firefox (2)
- VMware vCenter Server and Cloud Foundation
- Pulse Connect Secure
- Atlassian Jira Server and Data Center
- NETGEAR (2)
- Adobe (4)

The **full catalog** (downloadable in various formats) can be accessed here: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

*March 3, 2022*
*- by Jennifer Lyn Walker, Director of Infrastructure Cyber Defense*

It was only a matter of time before CISA posted a large cache of known exploited vulnerabilities in one day, today is that day. Today, **March 3, 2022**, CISA added a whopping **95 new vulnerabilities** to this catalog with CVE's ranging throughout the **last 20 years** that threat actors are **currently using to exploit systems that remain unpatched**. The vulnerabilities run the gamut of products, some with the earliest remediation due date of 3/17/2022.

Today's list includes **one industrial control product – Siemens SIMATIC CP 1543-1** with a CVE from 2016 (CVE-2016-8562) and remediation due date of 3/24/2022. As far as I can tell, this is the first ICS vulnerability to be included in the Known Exploited Vulnerabilities Catalog (again, it was only a matter of time).
Similarly, today includes the oldest vulnerability from 2002. It is for a component in Microsoft Windows NT and Windows 2000! In other words, a 20 year old vulnerability for 20+ year old operating systems that is CURRENTLY being exploited because the devices haven't been patched and are still in use/accessible. Perhaps it's a long lost device that no one realized was still connected to the network and therefore seems unimportant. But according to CISA, at least one bad actor found it, highlighting the importance of performing on-going and comprehensive asset inventories.

CISA's Known Exploited Vulnerabilities Catalog is a highly recommended resource to help all organizations prioritize patching and vulnerability mitigation. This **catalog now contains 478 vulnerabilities known to be currently used by threat actors to exploit devices that remain unpatched**. In addition, CISA includes remediation due dates which offer even more granularity in approaching and understanding the importance of patch prioritization and vulnerability mitigation. While the due dates are intended for federal networks, as always it is recommended that all organizations follow suit to best protect their environments.

Members are encouraged check the catalog and the regular updates for potentially impacted components in your environment. The importance of addressing known exploited vulnerabilities cannot be overstated and CISA has provided this great tool to help make this process less cumbersome.

The newly added vulnerabilities impact many well-known major products/vendors/platforms - please check the full catalog (sort by date added) to check for products used within your environment.

The **full catalog** (downloadable in various formats) can be accessed here: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

*March 1, 2022*

On February 25, 2022, CISA added **four** new vulnerabilities to this catalog with CVE's from 2014, 2017 (2), and 2022 that threat actors are currently using to exploit systems that remain unpatched. One of the vulnerabilities (Zimbra Webmail Cross-Site Scripting Vulnerability) has an upcoming remediation due date of 3/11/2022. Zimbra Webmail is reportedly used at more than a thousand government and financial institutions.

The newly added vulnerabilities impact the following products/vendors/platforms:

- Zimbra Webmail
- Microsoft Office
- Microsoft Internet Explorer
- Microsoft Windows