CISA's Known Exploited Vulnerabilities Catalog – April 2022 Archive

April 26, 2022
On **April 19 & 25, 2022**, CISA added **10** (3 and 7, respectively) new vulnerabilities to its Known Exploited Vulnerabilities Catalog. The 10 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 the recently standardized 3 week remediation deadline/address by due date of 5/10/2022 and 5/16/2022, respectively.

CISA's Known Exploited Vulnerabilities Catalog is a highly recommended resource to help all organizations prioritize patching. While the majority of the 654 entries (at the time of this post) impact IT environments, **there are currently 3 ICS/SCADA impacting vulnerabilities that threat actors are currently exploiting**.

For more guidance on improving patching, the National Cybersecurity Center of Excellence (NCCoE) has released two new final publications: Special Publication (SP) 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology and SP 1800-31, Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways.

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 **6** products/vendors/platforms:

- Jenkins
- Linux
- Meta Platforms
- Microsoft (5)
- WSO2
- Zimbra

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

The remaining posts will only list the details and other relevant bits of each addition to the catalog and not extra verbiage or references.

April 18, 2022
On **April 14 & 15, 2022**, CISA added **10** (1 and 9, respectively) new vulnerabilities to its Known Exploited Vulnerabilities Catalog. The 10 additions are for CVE's from 2007 – 2022 across **9** products that threat actors are currently using to exploit systems that remain unpatched. The new vulnerabilities have the seemingly recent standardized 3 week remediation deadline/address by due date of 5/5/2022 and 5/6/2022, respectively. Out of the 10, **2 of them are for old vulnerabilities from 2016 and 2018 impacting ICS/SCADA devices**, making a total of 3 ICS devices having been included in the catalog thus far (out of the 644 total vulnerabilities currently listed in the catalog).

The newly added vulnerabilities impact the following **9** products/vendors/platforms, **including 2 ICS/SCADA products**:

- Alcatel
- Crestron
- D-Link
- Google
- InduSoft
- **Schneider Electric** (CVE-2018-7841)
- **Trihedral** (CVE-2016-4523)
- Ubiquiti
- VMware (2)

April 14, 2022
On **April 13, 2022**, CISA **added 10 new vulnerabilities** to its Known Exploited Vulnerabilities Catalog. The 10 additions are for CVE's from 2014 – 2022 across 4 products that threat actors are currently using to exploit systems that remain unpatched. The new vulnerabilities have the seemingly recent standardized 3 week **remediation deadline/address by due date of 5/4/2022**. Out of the 10, 6 of them are for old vulnerabilities for Adobe Flash Player from 2014-2015 that are still running unpatched.

The newly added vulnerabilities impact the following **4** products/vendors/platforms:

- Adobe (6)
- Drupal
- Kaseya
- Microsoft (2)

April 12, 2022
On **April 11,2022**, CISA added **8 new** vulnerabilities to its Known Exploited Vulnerabilities Catalog. The 8 additions are for CVE's from 2017 – 2022 across 7 products that threat actors are currently using to exploit systems that remain unpatched. The new vulnerabilities have the seemingly recent standardized 3 week remediation deadline/address by due date of 5/2/2022. One of the vulnerabilities is for **WatchGuard Firebox and XTM firewall appliances** (CVE-2022-23176) that CISA has identified being exploited by the Russian state-sponsored threat group Sandworm as part the Cyclops Blink botnet infrastructure.

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

- Checkbox
- Google
- Microsoft (2)
- Linux
- QNAP
- Telerik
- WatchGuard (being exploited by Russian threat group Sandworm)

April 7, 2022
On **April 6,2022**, CISA added **3** new vulnerabilities to its Known Exploited Vulnerabilities Catalog. The 3 additions are for CVE's from 2017 – 2021 across **2 products** that threat actors are currently using to exploit systems that remain unpatched. The new vulnerabilities have the seemingly recent standardized 3 week remediation deadline/address by due date of 4/27/2022. Two of the vulnerabilities are for Microsoft products, including one from **2017 for a deprecated protocol, Microsoft SMBv1 Server**.

The newly added vulnerabilities impact the following 2 products/vendors/platforms:

- Microsoft (2)
- Sudo

April 5, 2022
On **April 4, 2022**, CISA added **4** new vulnerabilities to its Known Exploited Vulnerabilities Catalog. All 4 additions are for CVE's from 2021 – 2022 across 3 products that threat actors are currently using to exploit systems that remain unpatched. The new vulnerabilities have a remediation/address by due date of 4/25/2022, including a VMware update for the "Spring4Shell" vulnerability.

The newly added vulnerabilities impact the following **3** products/vendors/platforms:

- D-link
- Microsoft (2)
- VMware (update for "Spring4Shell")