CISA's Known Exploited Vulnerabilities Catalog – February 2022 Archive

February 24, 2022
On February 22, 2022, CISA added **two** new vulnerabilities to this catalog with current CVE's from 2022 that threat actors are currently using to exploit systems that remain unpatched. Both vulnerabilities impact Zabbix Frontend and have a remediation due date of 3/8/2022.

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 product/vendor/platform:

- Zabbix Frontend (2)

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

February 17, 2022
On February 15, 2022, CISA added **nine** new vulnerabilities to this catalog with **CVE's ranging from 2013 - 2022** that threat actors are currently using to exploit systems that remain unpatched. The most notable additions **include the following two recently addressed zero-days, both with a remediation due date of 3/1/2022:**

- a critical-severity vulnerability in Adobe Commerce and Magento (CVE-2022-24086)
- a high-severity security flaw impacting Google Chrome (CVE-2022-0609)

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 include the following products/vendors/platforms:

- Adobe (2)
- Google Chrome (1)
- Microsoft (4)
- PHPUnit (1)
- WinRAR (1)

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

February 15, 2022
On **February 10th and 11th, 2022**, CISA added **16 new vulnerabilities** to this catalog with **CVE's ranging from 2014 - 2022** that threat actors are currently using to exploit systems that remain unpatched. Two of the most *notable* recent additions include:

- an actively exploited zero-day for Apple iOS and macOS – Apple Webkit Remote Code Execution Vulnerability (CVE-2022-22620) with a pretty short address by date of 2/25/2022. While that date is for federal agencies, it's always recommended that all organizations follow suit.
- a Windows local privilege escalation vulnerability (CVE-2021-36934) dubbed HiveNightmare and SeriousSam

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

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

- Apache (2)
- Apple (3)
- D-Link (1)
- Jenkins (1)
- Microsoft (8)
- Oracle (1)

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

February 8, 2022
On February 4, 2022, CISA added 1 new vulnerability to this catalog. This flaw is a privilege escalation vulnerability affecting all unpatched versions of Windows 10 and requires zero user interaction to exploit. The vulnerability was addressed by Microsoft in January. As its addition to the aforementioned catalog indicates, it is being actively exploited in the wild. Given widespread use of Windows 10, CISA is urging this vulnerability be addressed by February 18, 2022.

The newly added vulnerability includes the following product/vendor/platform/component:

- Microsoft Win32k

Members are encouraged check the catalog and the regular updates for potentially impacted components in your environment and address accordingly to protect systems from exploitation.

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