CISA's Known Exploited Vulnerabilities Catalog – May 2022 Archive

May 26, 2022
On **May 25, 2022**, CISA added **34** vulnerabilities to its Known Exploited Vulnerabilities Catalog – making 75 for the week, so far. The **34 additions are ALL for older vulnerabilities** including CVE's from 2010 – 2019 across **7 vendors/projects** that threat actors are currently using to exploit systems that have not been patched yet. The new vulnerabilities have the standardized 3 week remediation deadline/address by due date of 6/15/2022.

Yesterday's 34 additions are notable due to the older age of the vulnerabilities across widely used enterprise products, including products that are end-of-life and still running in many production environments. These additions emphasize that threat actors are still scanning for, discovering, and subsequently exploiting older vulnerabilities. The importance of assessing your environment for potential impact and addressing these vulnerabilities accordingly cannot be over stated.

CISA's Known Exploited Vulnerabilities Catalog is a highly recommended resource to help all organizations prioritize patching. While the majority of the 737 entries impact IT environments, there are currently 3 ICS/SCADA impacting vulnerabilities that threat actors are currently exploiting.

For more guidance on improving patching, visit the National Cybersecurity Center of Excellence (NCCoE) for two 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 and address accordingly.

The newly added **34 vulnerabilities impact the following 7 vendors/projects:**
- Adobe (6)
- IBM
- Linux
- Microsoft (17)
- Mozilla
- Oracle (6)
- Red Hat (2)

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.

May 24, 2022 – During the **past 24 hours**, CISA **added 41 vulnerabilities** to its Known Exploited Vulnerabilities Catalog. The 41 additions are for CVE's from 2016 – 2022 across 12 vendors that threat actors are currently using to exploit systems that have not been patched yet. The new vulnerabilities have the standardized 3 week remediation deadline/address by due date of 6/13/2022 and 6/14/2022.

The newly added 41 vulnerabilities impact the following 12 vendors:
- Adobe
- Android (2)
- Apple (6)
- Artifex
- Cisco (3)
- Google (2)

- Kaseya
- Meta Platforms
- Microsoft (18)
- Mozilla (2)
- QNAP (3)
- WebKitGTK

May 17, 2022 – On **May 16, 2022**, CISA added **2 newly disclosed vulnerabilities** to its Known Exploited Vulnerabilities Catalog. The 2 additions are for CVE's from 2022 across **2 products** that threat actors are currently using to exploit systems that have not been patched yet. The new vulnerabilities have the standardized 3 week remediation deadline/address by due date of 6/6/2022.

Additionally, on May 13, 2022, due to issues with the vendor supplied update, the Microsoft Windows LSA Spoofing Vulnerability (that was added to the catalog last week) was temporarily removed. Please note there has been some confusion with the proper impacted CVE, but the importance is that even though it has been removed from the catalog does not mean that it isn't being exploited. Therefore, members are encouraged to follow the latest vendor guidance to protect systems until an effective patch is available. CISA Temporarily Removes CVE-2022-26925 from Known Exploited Vulnerability Catalog

The newly added (and subtracted) vulnerabilities impact the following products/vendors/platforms:

- VMware
- Zyxel
- TEMPORARILY Removed – Microsoft Windows LSA Spoofing Vulnerability

May 12, 2022 – On **May 10 and May 11, 2022**, CISA added **2 newly disclosed vulnerabilities** to its Known Exploited Vulnerabilities Catalog. The 2 additions are for CVE's from 2022 across **2 products** that threat actors are currently using to exploit systems that have not been patched yet. The new vulnerabilities have the recently standardized 3 week remediation deadline/address by due date of 5/31/2022 and 6/1/2022, respectively.

One of the additions is for the **critical vulnerability impacting F5 BIG-IP** that WaterISAC reported on in Tuesday's Security & Resilience Update, Critical Vulnerability Affecting F5 BIG-IP Requires Action. **If you use F5 BIG-IP,** please note that this is a very serious issue for those who have/had the management interface of the impacted appliances exposed to the internet. Cybersecurity experts are repeatedly urging companies to address this issue now and warning that if the management interface was exposed to the internet it is likely that the F5 has already been compromised. The Shadowserver Foundation has more guidance, but essentially, make sure to investigate for signs of compromise in accordance with best practices, do not expose your F5 management interface to the public Internet, and use firewalling to block traffic and make sure to patch your F5 system.

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

- F5 BIG-IP (F5 BIG-IP Missing Authentication Vulnerability)
- Microsoft (Microsoft Windows LSA Spoofing Vulnerability)

May 5, 2022 – On **May 4, 2022**, CISA added **5** new vulnerabilities to its Known Exploited Vulnerabilities Catalog. The 5 additions are for CVE's from 2014 – 2021 across **3** 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 5/25/2022.

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

- Apple (2)
- Microsoft (2)
- OpenSSL