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

***June 28, 2022***

On **June 27, 2022**, CISA added **8 vulnerabilities** to its *Known Exploited Vulnerabilities Catalog*. Most of the additions are for older vulnerabilities including **CVEs from 2018 – 2022** across 4 vendors/projects that threat actors are currently using to exploit systems that have not been patched yet. The new additions all have a 3 week remediation deadline/address by due date of 7/18/2022.

Yesterday's additions include 5 old vulnerabilities from 2018 – 2021 impacting multiple Apple products and a **previous zero-day exploit for a MiVoice Connect vulnerability** (CVE-2022-29499) which was exploited by attackers on a Linux-based Mitel MiVoice VoIP appliances prior to a patch being available to gain initial access in what is believed to be the beginning of a ransomware attack.

The newly added **8 vulnerabilities impact the following 4 vendors/projects**:

- Apple (5); with CVEs from 2018-2021
- Google
- Mitel
- Red Hat

While the majority of the 786 catalog entries impact IT environments, *there are currently 3 ICS/SCADA impacting vulnerabilities that threat actors are currently exploiting*. Furthermore, yesterday's additions are notable, once again, due to the older age of the vulnerabilities across widely used products. 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 older vulnerabilities accordingly cannot be over stated.

CISA's Known Exploited Vulnerabilities (KEV) Catalog is a highly recommended resource to help all organizations prioritize patching. To emphasize this process, CISA recently updated its KEV background page which corroborates the guidance that has been provided here on how organizations should use the KEV catalog as part of their vulnerability management program.

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

***June 16, 2022***

On **June 14, 2022**, CISA added the **Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (CVE-2022-30190), dubbed "Follina"** to its Known Exploited Vulnerabilities Catalog. The vulnerability was added after Microsoft officially announced release of a patch. The new addition has a 3 week remediation deadline/address by due date of 07/05/2022. Likewise, WaterISAC's Resource Center page on "Follina" has been updated accordingly.

While the majority of the 778 catalog entries impact IT environments, there are currently 3 ICS/SCADA impacting vulnerabilities that threat actors are currently exploiting.

***June 9, 2022***

On **June 8** and **June 9, 2022**, CISA added **39** vulnerabilities to its Known Exploited Vulnerabilities Catalog. Less one for 2022 and one for 2021, 37 of the additions are for older vulnerabilities including **CVE's from 2006 – 2019** across **8 vendors/projects** that threat actors are currently using to exploit systems that have not been patched yet. The new additions all have a 2 week remediation deadline/address by due date of 6/22/2022 and 6/23/2022, respectively.

While the majority of the 777 catalog entries impact IT environments, *there are currently 3 ICS/SCADA impacting vulnerabilities that threat actors are currently exploiting*. Furthermore, yesterday's additions are once again 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 older vulnerabilities accordingly cannot be over stated.

The newly added **39 vulnerabilities impact the following 8 vendors/projects**:

- Adobe (13)
- Microsoft (8)
- Cisco
- Google (8)
- NETGEAR
- Owl Labs (the only one from 2022 – CVE-2022-31460)
- QNAP (4)
- SAP (3)

***June 7, 2022***

On **June 2, 2022**, due to evidence of active exploitation, CISA added the recently disclosed vulnerability for Atlassian Confluence (CVE-2022-26134) to its Known Exploited Vulnerabilities Catalog. The vulnerability has an **immediate remediation deadline/address by due date of 6/6/2022**. Members using Atlassian Confluence are recommended to follow the vendor's latest guidance at Atlassian.

CISA's Known Exploited Vulnerabilities Catalog is a highly recommended resource to help all organizations prioritize patching. While the majority of the 738 entries impact IT environments, *there are currently 3 ICS/SCADA impacting vulnerabilities* that threat actors are currently exploiting.