CISA's Known Exploited Vulnerabilities Catalog – January 2022 Archive

February 1, 2022
On January 28, 2022, CISA added 8 new vulnerabilities to this catalog, all with **CVE's ranging from 2014 - 2022** that threat actors are currently using to exploit systems that remain unpatched.
Notably, the Microsoft Internet Explorer and GNU Bourne-Again Shell (Bash) vulnerabilities are from 2014. While hopefully you're not using Internet Explorer, clearly some organizations still are. That said, these recent updates indicate that threat actors are still exploiting the notorious 2014 "ShellShock" vulnerability for GNU Bourne-Again Shell (CVE-2014-6271).

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

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

- Apple
- SonicWall SMA 100 Appliances
- GNU Bourne-Again Shell (2) - both from 2014; 1 for "ShellShock"
- Microsoft Windows BITS
- Internet Explorer (2014)
- Grandstream Networks UCM6200 Series
- Intel Active Management Technology (AMT), Small Business Technology (SBT), and Standard Manageability

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

January 28, 2022
On January 21, 2022, CISA added 4 new vulnerabilities to this catalog, all with **CVE's ranging from 2006 - 2021** that threat actors are currently using to exploit systems that remain unpatched.

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

- Apache Struts (2)
- Microsoft Windows Win32k
- SolarWinds Serv-U

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

January 20, 2022
On January 19, 2022, CISA added 13 new vulnerabilities to this catalog, all with CVE's from 2020 and 2021 that threat actors are currently using to exploit systems that remain unpatched. The newly added vulnerabilities include the following products/vendors/platforms:

- October CMS
- Node.js
- vRealize Operations Manager API

- BIG-IP
- Nagios XI OS
- Microsoft Exchange Server
- Aviatrix Controller
- Drupal
- Apache Airflow
- Oracle Corporate Business Intelligence Enterprise Edition

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

January 12, 2022

In an effort to assist organizations in patching (and in response to Binding Operational Directive 22-01), starting in November 2021, CISA published and is maintaining a list of known vulnerabilities currently being exploited by threat actors. The Known Exploited Vulnerabilities Catalog contains vulnerabilities from 2010 (at the time of this writing) through the present day. Furthermore, the vulnerabilities on this list all have patches available. Unfortunately, many devices remain unpatched, thus providing an easy win for the bad guys. The catalog is regularly updated with vulnerabilities observed being actively and presently exploited. The catalog can be downloaded into a spreadsheet (or csv) and filtered/sorted by CVE, vendor, or product name, etc. for ease of identification against devices running in your environment. Each record contains a short description of the vulnerability and the spreadsheet can be customized/built-out and used to track patch status which could complement asset inventory and vulnerability management programs. The catalog is a prudent place to begin for reconciling products in your environment that may not have been patched against these currently exploited vulnerabilities. This catalog is a valuable tool for providing a quick-win validation against products used in your environment.

On **January 10, 2022, CISA added 15 new vulnerabilities** to this catalog, *including a vulnerabilities identified (and patched) in* ***2013 (Microsoft) and 2015 (IBM WebSphere)*** that threat actors are currently using to exploit systems that remain unpatched. The newly added vulnerabilities include the following products/vendors, including **two that are identified in AA22-011A being exploited by Russian state-sponsored threat actors***:

- VMware vCenter
- Hikvision
- FatPipe
- Google Chrome
- *Microsoft*
- Oracle WebLogic Server
- Fortinet FortiOS and FortiProxy
- Palo Alto PAN-OS
- **Exim MTA***
- *IBM WebSphere*
- Primetek Primefaces
- **Elastic Kibana***

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