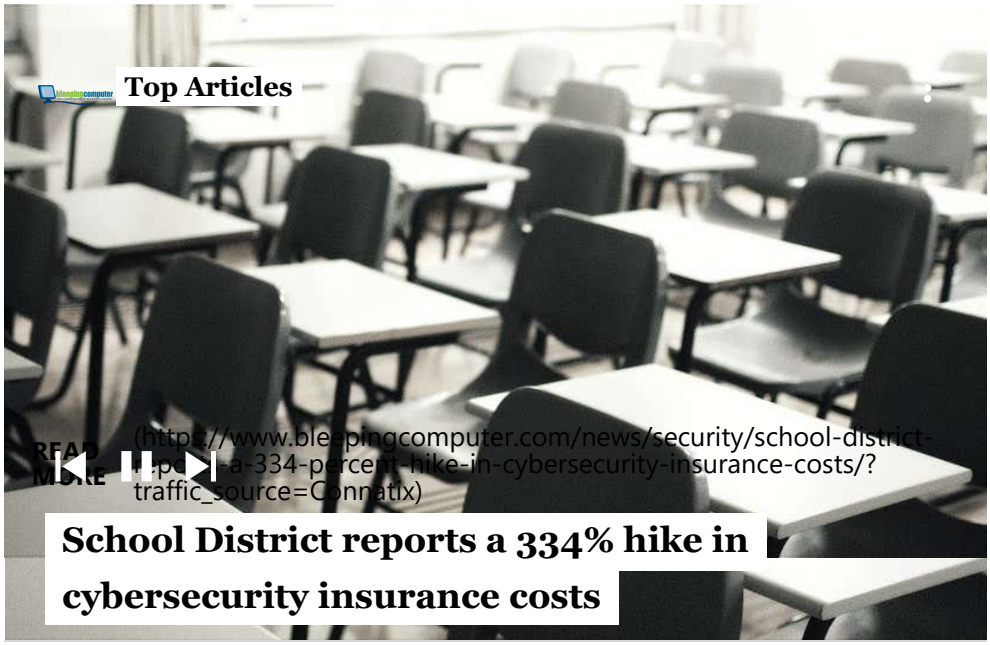
CISA adds 17 vulnerabilities to list of bugs exploited in attacks

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** January 22, 2022 03:36 PM **0**

This week, the Cybersecurity and Infrastructure Security Agency (CISA) added seventeen actively exploited vulnerabilities to the 'Known Exploited Vulnerabilities Catalog.

The 'Known Exploited Vulnerabilities Catalog' is a list of vulnerabilities that have been seen abused by threat actors in attacks and that are required to be patched by Federal Civilian Executive Branch (FCEB) agencies.

"Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities (https://cyber.dhs.gov/bod/22-01/) established the Known Exploited Vulnerabilities Catalog as a living list of known CVEs that carry significant risk to the federal enterprise," explains CISA.



"BOD 22-01 requires FCEB agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet (https://www.cisa.gov/known-exploited-vulnerabilities) for more information."

The vulnerabilities listed in the catalog allow threat actors to perform a variety of attacks, including stealing credentials, gaining access to networks, remotely executing commands, downloading and executing malware, or stealing information from devices.

With the addition of these 17 vulnerabilities, the catalog now contains a total of 341 vulnerabilities and includes the date by which agencies must apply security updates to resolve the bug.

The seventeen new vulnerabilities added this week are listed below, with CISA requiring 10 of them to be patched within the first week of February.

CVE Number	CVE Title	Required Action Due Date

CVE-2021-32648	October CMS Improper Authentication	2/1/2022
CVE-2021-21315	System Information Library for node.js Command Injection Vulnerability	2/1/2022
CVE-2021-21975	Server Side Request Forgery in vRealize Operations Manager API Vulnerability	2/1/2022
CVE-2021-22991	BIG-IP Traffic Microkernel Buffer Overflow Vulnerability	2/1/2022
CVE-2021-25296	Nagios XI OS Command Injection Vulnerability	2/1/2022
CVE-2021-25297	Nagios XI OS Command Injection Vulnerability	2/1/2022
CVE-2021-25298	Nagios XI OS Command Injection Vulnerability	2/1/2022
CVE-2021-33766	Microsoft Exchange Server Information Disclosure Vulnerability	2/1/2022
CVE-2021-40870	Aviatrix Controller Unrestricted Upload of File Vulnerability	2/1/2022
CVE-2021-35247	SolarWinds Serv-U Improper Input Validation Vulnerability	02/04/2022
CVE-2020-11978	Apache Airflow Command Injection Vulnerability	7/18/2022
CVE-2020-13671	Drupal Core Unrestricted Upload of File Vulnerability	7/18/2022
CVE-2020-13927	Apache Airflow Experimental API Authentication Bypass Vulnerability	7/18/2022
CVE-2020-14864	Oracle Corporate Business Intelligence Enterprise Edition Path Traversal Vulnerability	7/18/2022
CVE-2006-1547	Apache Struts 1 ActionForm Denial of Service Vulnerability	07/21/2022

CVE-2012-0391	Apache Struts 2 Improper Input Validation Vulnerability	07/21/2022
CVE-2018-8453	Microsoft Windows Win32k Privilege Escalation Vulnerability	07/21/2022

Of particular interest are the CVE-2021-32648 and CVE-2021-35247 vulnerabilities, which were disclosed this week to be actively exploited in attacks.

The 'October CMS Improper Authentication' vulnerability tracked as CVE-2021-32648 must be patched by February 1st, 2022, due to its recent use to hack and deface Ukrainian government websites (https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/).

While Ukraine blames these attacks on Russia (https://thedigital.gov.ua/news/rosiya-mae-namir-zniziti-doviru-do-vladi-feykami-pro-vrazlivist-kritichnoi-informatsiynoi-infrastrukturi-ta-zliv-danikh-ukraintsiv), some security experts attribute the attacks to a Belarus-tied hacking group known as Ghostwriter (https://www.mandiant.com/resources/unc1151-linked-to-belarus-government).

The new 'SolarWinds Serv-U Improper Input Validation' vulnerability tracked as CVE-2021-35247 was discovered by Microsoft to be exploited to propagate Log4j attacks (https://www.bleepingcomputer.com/news/microsoft/microsoft-solarwinds-fixes-serv-u-bug-exploited-for-log4j-attacks/) to Windows domain controllers configured as LDAP servers.

While attacks using the Serv-U vulnerability ultimately failed, as Windows domain controllers are not vulnerable to Log4j exploits, CISA requires agencies to fix the vulnerability by February 4th, 2022.

It is strongly recommended that all security professionals and admins review the Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) and patch any within their environment.