



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ALERT

CISA Adds Five Known Exploited Vulnerabilities to Catalog

Release Date: June 02, 2025

CISA added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog <<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>>, based on evidence of active exploitation.

- CVE-2021-32030 ASUS Routers Improper Authentication Vulnerability
- CVE-2023-39780 ASUS RT-AX55 Routers OS Command Injection Vulnerability
- CVE-2024-56145 Craft CMS Code Injection Vulnerability
- CVE-2025-3935 ConnectWise ScreenConnect Improper Authentication Vulnerability
- CVE-2025-35939 Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities <<https://www.cisa.gov/binding-operational-directive-22-01>> established the KEV Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (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/sites/default/files/publications/reducing_the_significant_risk_of_known_exploited_vulnerabilities_211103.pdf> for more information.

Although BOD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of [KEV Catalog vulnerabilities](#) <<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>> as part of their vulnerability management practice. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria <<https://www.cisa.gov/known-exploited-vulnerabilities>>.

Please share your thoughts with us through our [anonymous survey](#). We appreciate your feedback.

This product is provided subject to this [Notification](#) and this [Privacy & Use policy](#).

Please share your thoughts

We recently updated our anonymous [product survey](#); we'd welcome your feedback.

[Return to top](#)

Topics [</topics>](#) **Spotlight** [</spotlight>](#) **Resources & Tools** [</resources-tools>](#)

News & Events [</news-events>](#) **Careers** [</careers>](#) **About** [</about>](#)

CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA](#) [</about>](#)

[Budget and Performance](#)
<https://www.dhs.gov/performance-financial-reports>

[DHS.gov](https://www.dhs.gov) [</https://www.dhs.gov>](https://www.dhs.gov)

[FOIA Requests](https://www.dhs.gov/foia) [</https://www.dhs.gov/foia>](https://www.dhs.gov/foia) [No FEAR Act](#) [</no-fear-act>](#)

[Office of Inspector General](https://www.oig.dhs.gov/)
[</https://www.oig.dhs.gov/>](https://www.oig.dhs.gov/)

[Privacy Policy](#) [</privacy-policy>](#)

[Subscribe](#)

[The White House](#)
[</https://www.whitehouse.gov/>](https://www.whitehouse.gov/)

[USA.gov](https://www.usa.gov/) [</https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback](#) [</forms/feedback>](#)

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov