

CISA Identifies New Exploited Vulnerabilities: Action Required



CISA has added two vulnerabilities to its Known Exploited Vulnerabilities Catalog, indicating active exploitation. Organizations are advised to prioritize remediation efforts.

- Two new vulnerabilities added to CISA's KEV Catalog.
- CVE-2025-61624 affects multiple Fortinet products.
- CVE-2026-102764 involves BeyondTrust Remote Support.
- Organizations are encouraged to adopt risk-based vulnerability management.
- Rapid remediation of high-risk vulnerabilities is essential.

CISA has recently updated its Known Exploited Vulnerabilities (KEV) Catalog by adding two new vulnerabilities

that are currently being exploited. The first vulnerability, CVE-2025-61624, affects multiple products from Fortinet and involves a path traversal issue. The second, CVE-2026-102764, relates to an authentication bypass vulnerability in BeyondTrust Remote Support.

These vulnerabilities represent significant risks, particularly as they are frequently targeted by malicious cyber actors. CISA emphasizes the importance of prioritizing the remediation of these vulnerabilities, especially for organizations with publicly exposed assets that could allow for total control post-exploitation. While the Binding Operational Directive (BOD) 26-04 specifically applies to federal agencies, CISA encourages all organizations to adopt similar risk-based approaches to vulnerability management.

Organizations should remain vigilant and proactive in addressing vulnerabilities listed in the KEV Catalog. CISA will continue to update the catalog with new vulnerabilities that meet the criteria for active exploitation, and organizations are encouraged to report any known exploited vulnerabilities not currently listed.

What to do now

1. Review your systems for the listed vulnerabilities.
2. Prioritize remediation efforts for CVE-2025-61624 and CVE-2026-102764.
3. Implement a risk-based vulnerability management strategy.
4. Monitor CISA updates for new vulnerabilities.
5. Report any known exploited vulnerabilities not in the KEV Catalog.