

CISA adds six actively exploited vulnerabilities to KEV Catalog, including Plex, SiteGuard and Siemens flaws



CISA added six vulnerabilities in Plex Media Server, EG Secure Solutions SiteGuard Server Edition and Siemens Software Center to its KEV Catalog, citing evidence of active exploitation. It urges all organizations to prioritize them.

- Six CVEs were added to the KEV Catalog based on evidence of active exploitation.
- Four affect Plex Media Server: CVE-2026-96652, CVE-2026-96654, CVE-2026-96655 and CVE-2026-96656.
- CVE-2026-106931 is an OS command injection flaw in SiteGuard Server Edition; CVE-2026-110936 is an uncontrolled search path flaw in Siemens Software Center.
- BOD 26-04 binds only US federal civilian agencies, but CISA encourages every organization to adopt risk-based vulnerability management.

CISA has added six vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog after finding evidence that they are being exploited in the wild. CISA notes that flaws of these types are a frequent attack vector for malicious actors.

What was added

- CVE-2026-96652 and CVE-2026-96655: server-side request forgery (SSRF) in Plex Media Server
- CVE-2026-96654: improper neutralization of encoded URI schemes in a web page, Plex Media Server
- CVE-2026-96656: external control of file name or path, Plex Media Server
- CVE-2026-106931: OS command injection in EG Secure Solutions SiteGuard Server Edition
- CVE-2026-110936: uncontrolled search path element in Siemens Software Center

The source does not provide patch details or affected versions, so refer to each vendor's advisory for those.

Why it matters beyond US agencies

CISA's Binding Operational Directive (BOD) 26-04 requires federal civilian agencies to prioritize fast remediation of KEV-listed CVEs on publicly exposed assets where exploitation gives full control of the asset. It also sets basic expectations for checking whether a system was compromised before the patch was applied. The directive applies only to those agencies, yet CISA encourages all organizations to adopt risk-based vulnerability management and to prioritize KEV Catalog entries.

Suggested approach

Treat KEV listing as a strong signal of real-world exploitation. Confirm whether the affected products exist in your environment, including in less visible places such as shadow IT or engineering workstations, and sequence remediation by exposure first.

What to do now

1. Check asset inventories for Plex Media Server, SiteGuard Server Edition and Siemens Software Center.
2. Review each vendor's advisory and apply available patches or mitigations, starting with internet-exposed systems.
3. If a vulnerable system was exposed before patching, review logs and look for signs of compromise.
4. Add KEV Catalog monitoring to your vulnerability management process and prioritize listed CVEs.
5. Remove or isolate unneeded media-server software from corporate networks.