

## CISA flags OS command injection flaw in EG Secure Solutions SiteGuard Server Edition (CVE-2026-106931)



CISA lists an OS command injection flaw, CVE-2026-106931, in SiteGuard Server Edition that could let an attacker run commands with root or SYSTEM privileges. Vendor mitigations should be applied and exposure reviewed.

- CVE-2026-106931 is an OS command injection vulnerability in EG Secure Solutions SiteGuard Server Edition.
- Successful exploitation may allow arbitrary OS commands with root or SYSTEM privileges on the host.
- CISA requires mitigations per vendor instructions, in line with BOD 26-04 and its Forensics Triage Requirements.
- If mitigations are unavailable, CISA's guidance is to discontinue use of the product.

- The federal due date is 2026-10-23; each organisation must assess the internet exposure of its own assets.

CISA has added CVE-2026-106931 to its catalogue of vulnerabilities. It is an OS command injection flaw in EG Secure Solutions SiteGuard Server Edition.

## What the flaw allows

According to the source, an attacker who exploits the flaw may be able to execute arbitrary operating system commands with root or SYSTEM privileges on the system that runs the product. That level of access means the host itself could be fully affected, not only the application.

## What CISA requires

CISA asks organisations to apply mitigations in accordance with the vendor's instructions, and to follow its BOD 26-04 guidance on prioritising security updates based on risk. It also refers to its Forensics Triage Requirements. Where mitigations are not available, the guidance is to discontinue use of the product. For cloud services, the applicable BOD 26-04 guidance should be followed. The federal due date is 2026-10-23.

The source places responsibility on each organisation to evaluate the internet exposure of every asset and to adhere to the patching guidelines. The source does not name affected versions or fixed releases, so these should be confirmed directly with the vendor.

## Practical view for Saudi institutions

The CISA due date applies to US federal agencies, but the guidance is a sensible benchmark for any regulated institution that runs this product. Start by establishing whether SiteGuard Server Edition is present in your environment and whether it is reachable from the internet.

## What to do now

1. Check asset inventories and scanners for any SiteGuard Server Edition deployment.
2. Determine which instances are reachable from the internet and prioritise them.
3. Contact EG Secure Solutions for mitigation instructions and affected-version details, and apply them.
4. If no mitigation is available, plan to discontinue use of the product, as CISA advises.
5. Review logs and preserve evidence on exposed hosts to support a forensic triage if compromise is suspected.