GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

21 October 2026

Advisory 362: SiteGuard Server Edition OS Command Injection Vulnerability in the Statistics Feature - Confirmed Exploited (CVE-2026-106931).

Release Date: 20th October 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-106931 is an OS command injection vulnerability (CWE-78) in the statistics feature of SiteGuard Server Edition, a web application firewall module that runs on web servers. An attacker who exploits it can run arbitrary operating system commands with root privileges (Linux and FreeBSD) or SYSTEM privileges (Windows IIS).

What are the systems affected?

SiteGuard Server Edition Ver 2.20 and later is affected when the statistics feature is enabled, which is the default:

- SiteGuard Server Edition for Apache httpd, Nginx and IIS: versions before Ver 8.00 Update 5
- SiteGuard Server Edition for Apache httpd and Nginx on FreeBSD: versions before Ver 7.00 Update 6

Not affected / patched version:

- Ver 8.00 Update 5 for Apache httpd, Nginx and IIS
- Ver 7.00 Update 6 for Apache httpd and Nginx on FreeBSD
- IIS Ver 3.10 to Ver 4.00 Update 4 are not affected

- Users who cannot upgrade can apply the vendor's patch, which replaces the files used in statistical processing. It is also available for end-of-support versions

What does this mean?

Successful exploitation may allow attackers to:

- Run arbitrary operating system commands with root or SYSTEM privileges on the web server
- Take over the web server and disable or bypass the web application firewall protecting hosted applications
- Steal data and credentials from the server and use it as a foothold into the network

Mitigation process

CERTVU recommends the following:

1. Preserve evidence first
Before updating or patching, download the diagnostic information from the web admin console (Diagnostics > Download Diagnostic Information) and keep it. The vendor warns that updating may erase evidence of attacks.

2. Update or apply the vendor patch
Update to Ver 8.00 Update 5 (or Ver 7.00 Update 6 on FreeBSD). If an update is not possible, apply the vendor patch that replaces the statistics processing files, including on end-of-support versions. Contact your support desk or reseller, or JPCERT/CC, for the patch.

3. Hunt for compromise
4. Limit access to the host
5. Rotate credentials

If compromise is suspected, rotate credentials and keys held on the server, and report the incident to CERTVU.

Reference

1. https://jvn.jp/en/jp/JVN88474777/
2. https://www.eg-secure.co.jp/siteguard/news/alert-202610-1
3. https://www.thehackerwire.com/vulnerability/CVE-2026-106931/
4. https://nvd.nist.gov/vuln/detail/CVE-2026-106931