contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

EG Secure Solutions SiteGuard Server Edition exploited

CVE-2026-106931 · on CISA's exploited list since 20 October 2026

Analysis Report

If you run SiteGuard Server Edition Ver2.20 or later with the statistics feature on, act now, because CISA's deadline has passed. First download the diagnostic information, then update or apply the …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 4.0 8.5**	STATUS	On CISA's exploited list; due 23 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/eg-secure-solutions-siteguard-server-edition-cve-2026-106931

The bottom line

> *If you run SiteGuard Server Edition Ver2.20 or later with the statistics feature on, act now, because CISA's deadline has passed. First download the diagnostic information, then update or apply the vendor's patch. If you do not run it, you can stop reading.*

At a glance

Fact	Detail
Product	EG Secure Solutions SiteGuard Server Edition (CVE-2026-106931)
Severity	High: 8.5 (CVSS 4.0)
CISA	On its exploited list since 20 October 2026. Deadline for US federal agencies: 23 October 2026.
Chance of exploitation (EPSS)	0.03, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Ver8.00 Update5 (Apache, Nginx, IIS, not FreeBSD); Ver7.00 Update6 (FreeBSD Apache and Nginx). Source: vendor notice, 14 October 2026.
Who looks first	Anyone who runs SiteGuard Server Edition Ver2.20 or later on a web server (Apache, Nginx, IIS or FreeBSD) with the statistics feature on. It is on by default.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run SiteGuard Server Edition, the host-based web application firewall, on any web server?	Nothing to do for this CVE.	Check the version (next question).
Is it Ver2.20 or later, and older than the fixed version for your web server?	Not affected by the ranges given. Note IIS Ver3.10 to Ver4.00 Update4 is also unaffected.	Check whether the statistics feature is on.
Is the statistics feature enabled (it is on by default)?	The vendor says the flaw applies only when it is on. Still plan the update.	Save the diagnostic information, then patch.

Can anyone untrusted log in to, or run code on, the server?	Lower chance of use, but the vendor says attacks have been confirmed.	Treat as urgent and look for signs of misuse.

What it is

A flaw in the statistics feature lets an attacker run any operating system command with root or SYSTEM rights on the server that runs the product. The scores say the attacker needs local access and a low-privilege account first.

Why it matters

The vendor and JVN both say exploitation has been confirmed. Our reading is that the score of 8.5 understates the risk: the attacker needs a foothold first, but the result is full control of the server that sits in front of your website. A web application firewall host is a good place to hide, so a foothold from another flaw could become complete takeover through this one.

What the vendor's advisory says

We read two pages on www.eg-secure.co.jp and jvn.jp. In short:

- The vendor's notice says exploitation is confirmed and rates the flaw as urgent.
- The vendor says customers with direct support contracts were told on 29 September 2026.
- The vendor says updating or patching can erase traces of an attack, so download the diagnostic information first.
- The vendor offers a patch that replaces the statistics processing files for those who cannot upgrade, including unsupported versions.
- The vendor gives the diagnostic download path as: web admin screen, Diagnostic information, Download diagnostic information.

Things people will get wrong

- "It needs a login, so it can wait." The vendor says it is already exploited, and the result is root or SYSTEM control. Any foothold from another flaw is enough to start.
- "Our version is old and out of support, so no fix exists." The vendor says its patch is available even for end-of-life versions.
- "Updating first is the safest move." The vendor warns that updating or patching can erase traces of an attack. Save the diagnostic information first.

The wording includes conditions the score may not show: it needs privileges. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the versions you run

- List every server running SiteGuard Server Edition and note the web server type (Apache, Nginx, IIS, FreeBSD).
- Compare each with Ver8.00 Update5, or Ver7.00 Update6 on FreeBSD.

```
dpkg -l | grep -i siteguard
rpm -qa | grep -i siteguard
```

Step 2: Save evidence before changing anything

- In the web admin screen, download the diagnostic information and store it off the server.
- The vendor says an update or patch can erase attack traces.

Step 3: Update or patch

- Update to the fixed version for your web server.
- If you cannot upgrade, ask the vendor or your reseller for the patch for the statistics processing files.

Step 4: Check the result

- Confirm the version afterwards and keep the diagnostic file with your records.
- Ask your provider to review the saved information for signs of misuse.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to check our exposure to CVE-2026-106931, an OS command injection flaw in the statistics feature of SiteGuard Server Edition (Ver2.20 and later). The vendor says it is being exploited. Please tell us whether we run this product, on which servers, which version, and whether statistics is on. Before any change, please download and keep the diagnostic information. Then please update to Ver8.00 Update5 (Ver7.00 Update6 on FreeBSD) or apply the vendor's patch. Please confirm the version and the fix in writing by the end of this week.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Anything unexpected in the diagnostic information the product produces, saved before patching.
- New or changed accounts, scheduled tasks or services on the server since September 2026.
- Unexpected commands or processes started by the statistics feature or by the web server's account.

The weakness behind it

The record classes this as CWE-78 (Improper Neutralization of Special Elements used in an OS Command).

The sources, in their words

CISA's catalogue entry:

> *EG Secure Solutions SiteGuard Server Edition contains an OS command injection vulnerability which may allow an attacker to execute arbitrary OS commands with root or SYSTEM privileges on the system running the affected product.*

The CVE record, published by Jpcert on 14 October 2026:

> *SiteGuard Server Edition contains an OS command injection vulnerability, which may allow an attacker to execute arbitrary OS commands with root or SYSTEM privileges on the system running the affected product.*

Versions of EG Secure Solutions Inc. SiteGuard Server Edition for Apache httpd the record lists as affected:

- Ver2.20 up to, but not including, Ver8.00 Update 5

The affected ranges end before Ver8.00 Update 5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of EG Secure Solutions Inc. SiteGuard Server Edition for Nginx the record lists as affected:

- Ver2.20 up to, but not including, Ver8.00 Update 5

The affected ranges end before Ver8.00 Update 5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of EG Secure Solutions Inc. SiteGuard Server Edition for IIS the record lists as affected:

- Ver2.20 up to, but not including, Ver8.00 Update 5

The affected ranges end before Ver8.00 Update 5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of EG Secure Solutions Inc. SiteGuard Server Edition for Apache httpd on FreeBSD the record lists as affected:

- Ver2.20 up to, but not including, Ver7.00 Update 6

The affected ranges end before Ver7.00 Update 6. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Whether the sources say how attackers get the low-privilege access the scores require.
- What the attacks look like, or who is being targeted.
- Whether the vendor patch is as complete as the update; the sources do not compare them.
- Whether Nginx on FreeBSD is covered by the record's affected list; the vendor notice lists it, the record lists only Apache.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it"

and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-106931: score 8.5, `CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Local	Needs an account or code already running on the machine.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	None	No data exposed.
Subsequent systems: integrity	None	Nothing can be altered.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
14 October 2026	CVE record published by Jpcert.
20 October 2026	CISA added it to its list of exploited vulnerabilities.
23 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Affected version, statistics on, and the server hosts other users or untrusted accounts	High	Now; CISA's window has passed

Affected version, statistics on, only trusted administrators have access	High	Now; exploitation is confirmed
Affected version with statistics switched off	Medium	Next patch cycle
End-of-life version that cannot be upgraded	High	This week, using the vendor's patch
Fixed version already installed, or product not used	None	None for this CVE

Appendix 4. Definition of done

- Every EG Secure Solutions SiteGuard Server Edition you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-106931: https://www.cve.org/CVERecord?id=CVE-2026-106931
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.eg-secure.co.jp/siteguard/news/alert-202610-1: https://www.eg-secure.co.jp/siteguard/news/alert-202610-1
- Advisory or release notes read: jvn.jp/en/jp/JVN88474777/: https://jvn.jp/en/jp/JVN88474777/