STORMSHIELD

Search for... Submit

Stored XSS in the VPN logs monitor

Stored XSS in the VPN logs monitor

Advisory ID	CVE Number	Date discovered	Severity	Advisory revision
STORM-2026-030	CVE-2026-111088	09/30/2026	high	v1

Vulnerability details

A Stored Cross-Site Scripting vulnerability exists in the SNS VPN log monitoring screen.

Impacted products

Products	Severity	Detail
Stormshield Network Security	high	SNS is impacted.

Revisions

Version	Date	Description
v1	10/16/2026	Initial release
v2	10/20/2026	Advisory disclosure

Stormshield Network Security | **CVSS v3.1 Overall Score: 7.5**

Analysis

In some cases, the SSL VPN monitoring component does not sanitize some log fields.

Impacted version

- SNS 5.1.0 to 5.1.3
- SNS 5.0.0 to 5.0.9
- SNS 4.8.0 to 4.8.19
- SNS 4.3.0 to 4.3.44

Workaround solution

There is no workaround solution.

Solution

The following updates will fix this vulnerability:

- SNS 5.1.4 EA
- SNS 5.0.10
- SNS 4.8.20 LTSB
- SNS 4.3.45 QS

Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Confidentiality Impact	Integrity Impact	Availability impact
Network	Low	Low	None	Unchanged	High	None	None

CVSS Base score: 6.5 CVSS Vector: (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

Exploit Code Maturity	Remediation Level	Report Confidence
Proof of concept code	Official fix	Confirmed

CVSS Temporal score: 5.9 CVSS Vector: (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C)

Confidentiality Requirement (CR)	Integrity Requirement (IR)	Availability Requirement (AR)
High	Low	Low

CVSS Environmental score: 7.5 CVSS Vector: (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C/CR:H/IR:L/AR:L/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X)

RSS Feed

Should you encounter any problem, please contact your Stormshield Technical Assistance Center