



CVE-2018-9866

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-9866
State	PUBLIC
Assigner	PSIRT@sonicwall.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-03 20:29:00 UTC
Updated	2019-10-09 23:43:00 UTC
Description	A vulnerability in lack of validation of user-supplied parameters pass to XML-RPC calls on SonicWall Global Management S

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonicwall	Global Management System	All	All	All	All

References

Reference
Security Advisory
Add SonicWall XML-RPC Remote Code Execution Exploit Module by Flandini · Pull Request #10305 · rapid7/metasploit-framework · GitHub
Davy Douhine na Twitterze: "Want to pwn SonicWall firewalls ? Get a root shell with this upcoming #metasploit exploit (written by Michael Flar
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)