



CVE-2021-20026

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

Summary

CVE	CVE-2021-20026
State	PUBLIC
Assigner	PSIRT@sonicwall.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-27 19:15:00 UTC
Updated	2021-06-08 16:36:00 UTC
Description	A vulnerability in the SonicWall NSM On-Prem product allows an authenticated attacker to perform OS command injection u

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonicwall	Network Security Manager	All	All	All	All
Application	Sonicwall	Network Security Manager	2.2.0	-	All	All
Application	Sonicwall	Network Security Manager	2.2.0	r10	All	All

References

Reference	Source	Link	Tags
Security Advisory	CONFIRM	psirt.global.sonicwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375597](#) SonicWall Network Security Manager Authenticated Command Injection Vulnerability (SNWLID-2021-0014)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)