



CVE-2021-20038

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

Summary

CVE	CVE-2021-20038
State	PUBLIC
Assigner	PSIRT@sonicwall.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-08 10:15:00 UTC
Updated	2022-05-13 14:54:00 UTC
Description	A Stack-based buffer overflow vulnerability in SMA100 Apache httpd server's mod_cgi module environment variables allow

Risk And Classification

EPSS: 0.942920000 probability, percentile 0.999420000 (date 2026-04-02)

CISA KEV: Listed on 2022-01-28; due 2022-02-11; ransomware use Known

Problem Types: CWE-787

CISA Known Exploited Vulnerability

Vendor	SonicWall
Product	SMA 100 Appliances
Name	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-20038

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sonicwall	Sma 200	-	All	All	All
Operating System	Sonicwall	Sma 200 Firmware	10.2.0.8-37sv	All	All	All
Operating System	Sonicwall	Sma 200 Firmware	10.2.1.1-19sv	All	All	All
Operating System	Sonicwall	Sma 200 Firmware	10.2.1.2-24sv	All	All	All
Hardware	Sonicwall	Sma 210	-	All	All	All
Operating System	Sonicwall	Sma 210 Firmware	10.2.0.8-37sv	All	All	All
Operating System	Sonicwall	Sma 210 Firmware	10.2.1.1-19sv	All	All	All
Operating System	Sonicwall	Sma 210 Firmware	10.2.1.2-24sv	All	All	All

Hardware	Sonicwall	Sma 400	-	All	All	All
Operating System	Sonicwall	Sma 400 Firmware	10.2.0.8-37sv	All	All	All
Operating System	Sonicwall	Sma 400 Firmware	10.2.1.1-19sv	All	All	All
Operating System	Sonicwall	Sma 400 Firmware	10.2.1.2-24sv	All	All	All
Hardware	Sonicwall	Sma 410	-	All	All	All
Operating System	Sonicwall	Sma 410 Firmware	10.2.0.8-37sv	All	All	All
Operating System	Sonicwall	Sma 410 Firmware	10.2.1.1-19sv	All	All	All
Operating System	Sonicwall	Sma 410 Firmware	10.2.1.2-24sv	All	All	All
Hardware	Sonicwall	Sma 500v	-	All	All	All
Operating System	Sonicwall	Sma 500v Firmware	10.2.0.8-37sv	All	All	All
Operating System	Sonicwall	Sma 500v Firmware	10.2.1.1-19sv	All	All	All
Operating System	Sonicwall	Sma 500v Firmware	10.2.1.2-24sv	All	All	All

References

Reference	Source	Link	Tags
GitHub - jbaines-r7/badblood: SonicWall SMA-100 Unauth RCE Exploit (CVE-2021-20038)	MISC	github.com	
Security Advisory	CONFIRM	psirt.global.sonicwall.com	
CVE-2021-20038..42: SonicWall SMA 100 Multiple Vulnerabilities (FIXED) Rapid7 Blog	MISC	www.rapid7.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730337](#) SonicWall Secure Mobile Access 100 Multiple Vulnerabilities (SNWLID-2021-0026)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)