



CVE-2023-30806

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

Summary

CVE	CVE-2023-30806
State	PUBLIC
Assigner	disclosure@vulncheck.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-10 15:15:00 UTC
Updated	2023-10-13 15:00:00 UTC
Description	The Sangfor Next-Gen Application Firewall version NGAF8.0.17 is vulnerable to an operating system command injection vul

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sangfor	Next-gen Application Firewall	ngaf8.0.17	All	All	All

References

Reference	Source	Link	Tags
Yet More Unauth Remote Command Execution Vulns in Firewalls - Sangfor Edition	MISC	labs.watchtower.com	
Sangfor Next-Gen Application Firewall PHPSESSID Command Injection VulnCheck Advisories	MISC	vulncheck.com	
AWS Marketplace: Sangfor Next-Gen Application Firewall	MISC	aws.amazon.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730975](#) Sangfor Next-Generation Application Firewall (NGAF) Multiple Vulnerabilities

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report