CVE-2019-19356

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-19356
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-07 23:15:00 UTC
Updated	2022-01-01 19:57:00 UTC
Description	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management p

Risk And Classification

EPSS: 0.910880000 probability, percentile 0.996490000 (date 2026-04-28)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	Netis
Product	WF2419 Devices
Name	Netis WF2419 Devices Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-19356

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netis-systems	Wf2419	-	All	All	All
Hardware	Netis-systems	Wf2419	-	All	All	All
Operating System	Netis-systems	Wf2419 Firmware	1.2.31805	All	All	All
Operating System	Netis-systems	Wf2419 Firmware	2.2.36123	All	All	All
Operating System	Netis-systems	Wf2419 Firmware	1.2.31805	All	All	All
Operating System	Netis-systems	Wf2419 Firmware	2.2.36123	All	All	All

References

Reference	Source	Link	Tags
Netis Routers - Remote Code Execution (CVE-2019-19356) | Digital Security	MISC	www.digital.security	Exploit, Third
GitHub - shadowgatt/CVE-2019-19356: Netis router RCE exploit (CVE-2019-19356)	MISC	github.com	
Netis WF2419 2.2.36123 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730378 Netis WF2419 Remote Code Execution (RCE) Vulnerability

Free CVE JSON API cve.report/api

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