

CVE-2021-20090

Arcadyan Buffalo Firmware Path Traversal Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

A path traversal vulnerability in the web interfaces of Buffalo WSR-2533DHPL2 firmware version ≤ 1.02 and WSR-2533DHP3 firmware version ≤ 1.24 could allow unauthenticated remote attackers to bypass authentication.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
wsr-2533dhpl2-bk firmware	≤ 1.02	after 1.02	NVD
wsr-2533dhp3-bk firmware	≤ 1.24	after 1.24	NVD
wsr-2533dhpl2-bk	—	no fixed version listed	NVD
wsr-2533dhp3-bk	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-6466-44wr-c6vv	NVD	nvd.nist.gov/vuln/detail/CVE-2021-20090
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-7547
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-20090		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.