

CVE-2022-30525

Zyxel Multiple Firewalls OS Command Injection Vulnerability

Exigent

CISA KEV since May 16, 2022

Actively exploited

Public exploit module (Metasploit)

A OS command injection vulnerability in the CGI program of Zyxel USG FLEX 100(W) firmware versions 5.00 through 5.21 Patch 1, USG FLEX 200 firmware versions 5.00 through 5.21 Patch 1, USG FLEX 500 firmware versions 5.00 through 5.21 Patch 1, USG FLEX 700 firmware versions 5.00 through 5.21 Patch 1, USG FLEX 50(W) firmware versions 5.10 through 5.21 Patch 1, USG20(W)-VPN firmware versions 5.10 through 5.21 Patch 1, ATP series firmware versions 5.10 through 5.21 Patch 1, VPN series firmware versions 4.60 through 5.21

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Jun 6, 2022 KEV since 2022 · 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

Patch 1, which could allow an attacker to modify specific files and then execute some OS commands on a vulnerable device.

Affected and fixed versions · 24 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
usg flex 100w firmware	≥ 5.00 < 5.30	5.30	NVD
usg flex 200 firmware	≥ 5.00 < 5.30	5.30	NVD
usg flex 500 firmware	≥ 5.00 ≤ 5.30	after 5.30	NVD
usg flex 700 firmware	≥ 5.00 < 5.30	5.30	NVD
vpn100 firmware	≥ 4.60 < 5.30	5.30	NVD
vpn1000 firmware	≥ 4.60 < 5.30	5.30	NVD
vpn300 firmware	≥ 4.60 < 5.30	no fixed version listed	NVD
vpn50 firmware	≥ 4.60 < 5.30	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-987m-9prq-3p7m

Additional guidance zyxel.com/support/Zyxel-security-advisory-for-OS-command-injection-vulnerability-of-firewalls.shtml

NVD nvd.nist.gov/vuln/detail/CVE-2022-30525

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-52385

Current data evulnable.com/vulnerability-management/cve/CVE-2022-30525

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