

CVE-2023-28771

Zyxel Multiple Firewalls OS Command Injection Vulnerability

Exigent

CISA KEV since May 31, 2023

Actively exploited

Public exploit module (Metasploit)

Improper error message handling in Zyxel ZyWALL/USG series firmware versions 4.60 through 4.73, VPN series firmware versions 4.60 through 5.35, USG FLEX series firmware versions 4.60 through 5.35, and ATP series firmware versions 4.60 through 5.35, which could allow an unauthenticated attacker to execute some OS commands remotely by sending crafted packets to an affected device.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.993 99.94th percentile · FIRST	CISA DEADLINE Jun 21, 2023 KEV since 2023 · 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	0.993 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 · 30 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
atp100 firmware	≥ 4.60 < 5.36	5.36	NVD
atp100w firmware	≥ 4.60 < 5.35	5.35	NVD
atp200 firmware	≥ 4.60 < 5.36	5.36	NVD
atp500 firmware	≥ 4.60 < 5.36	5.36	NVD
atp700 firmware	≥ 4.60 < 5.36	5.36	NVD
atp800 firmware	≥ 4.60 < 5.36	5.36	NVD
usg flex 100 firmware	≥ 4.60 < 5.36	no fixed version listed	NVD
usg flex 100w firmware	≥ 4.60 < 5.36	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-3xvp-8qg2-x43w

Additional guidance zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls

NVD nvd.nist.gov/vuln/detail/CVE-2023-28771

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-32406

Current data evulnable.com/vulnerability-management/cve/CVE-2023-28771

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