



CVE-2021-35028

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

Summary

CVE	CVE-2021-35028
State	PUBLIC
Assigner	security@zyxel.com.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-29 11:15:00 UTC
Updated	2021-10-02 15:18:00 UTC
Description	A command injection vulnerability in the CGI program of the Zyxel VPN2S firmware version 1.12 could allow an authenticat

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Zyxel	Zywall Vpn2s	-	All	All	All
Operating System	Zyxel	Zywall Vpn2s Firmware	1.12\(\abln.0\)c0	All	All	All

References

Reference	Source	Link	Tags
404 Error Zyxel	MISC	www.zyxel.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)