



CVE-2021-4029

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

Summary

CVE	CVE-2021-4029
State	PUBLIC
Assigner	security@zyxel.com.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-24 15:15:00 UTC
Updated	2022-03-02 15:46:00 UTC
Description	A command injection vulnerability in the CGI program of the Zyxel ARMOR Z1/Z2 firmware could allow an attacker to execute

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Zyxel	Nbg6816	-	All	All	All
Operating System	Zyxel	Nbg6816 Firmware	1.00\(\aawb.10\)c0	All	All	All
Hardware	Zyxel	Nbg6817	-	All	All	All
Operating System	Zyxel	Nbg6817 Firmware	All	All	All	All

References

Reference	Source
Zyxel security advisory for command injection and cross-site request forgery vulnerabilities of select Armor home routers Zyxel	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)