



CVE-2022-45440

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

Summary

CVE	CVE-2022-45440
State	PUBLIC
Assigner	security@zyxel.com.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-17 02:15:00 UTC
Updated	2023-07-07 18:42:00 UTC
Description	A vulnerability exists in the FTP server of the Zyxel AX7501-B0 firmware prior to V5.17(ABPC.3)C0, which processes symb

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Zyxel	Ax7501-b0	-	All	All	All
Operating System	Zyxel	Ax7501-b0 Firmware	All	All	All	All

References

Reference	Score
Zyxel security advisory for cleartext storage of WiFi credentials and improper symbolic links of FTP for AX7501-B0 CPE Zyxel Networks	CC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report