



CVE-2015-7284

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

Summary

CVE	CVE-2015-7284
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-31 05:59:00 UTC
Updated	2016-12-07 18:23:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability on ZyXEL NBG-418N devices with firmware 1.00(AADZ.3)C0 allows remote

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Zyxel	Nbg-418n	All	All	All	All
Hardware	Zyxel	Nbg-418n	All	All	All	All
Operating System	Zyxel	Nbg-418n Firmware	1.00(aadz.3)c0	All	All	All
Operating System	Zyxel	Nbg-418n Firmware	1.00(aadz.3)c0	All	All	All
Operating System	Zyxel	Nbg-418n Firmware	1.00(aadz.3)c0	All	All	All

References

Reference

ZyXEL NBG-418N Router Insecure Default Password and Cross Site Request Forgery vulnerabilities
Vulnerability Note VU#330000 - ZyXEL NBG-418N router uses default credentials and is vulnerable to cross-site request forgery
ZyXEL NBG-418N Wireless Router Bugs Let Remote Users Conduct Cross-Site Request Forgery Attacks and Gain Administrative Access - S
CVE Program record
NVD vulnerability detail

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](#).

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