



# CVE-2023-22923

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

## Summary

<b>CVE</b>	CVE-2023-22923
<b>State</b>	PUBLIC
<b>Assigner</b>	security@zyxel.com.tw
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-01 17:15:00 UTC
<b>Updated</b>	2023-05-06 03:11:00 UTC
<b>Description</b>	A format string vulnerability in a binary of the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow

## Risk And Classification

**Problem Types:** CWE-134

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Zyxel</a>	Nbg-418n	v2	All	All	All
Operating System	<a href="#">Zyxel</a>	Nbg-418n Firmware	All	All	All	All

## References

Reference	Source	Link	Tags
Page Not Found   Zyxel Networks	CONFIRM	<a href="http://www.zyxel.com">www.zyxel.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	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](#)**