



CVE-2023-27989

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-27989
State	PUBLIC
Assigner	security@zyxel.com.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-05 12:15:00 UTC
Updated	2023-06-12 16:50:00 UTC
Description	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could e

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Zyxel	Lte7480-m804	-	All	All	All
Operating System	Zyxel	Lte7480-m804 Firmware	All	All	All	All
Hardware	Zyxel	Lte7490-m904	-	All	All	All
Operating System	Zyxel	Lte7490-m904 Firmware	All	All	All	All
Hardware	Zyxel	Nebula Nr7101	-	All	All	All
Operating System	Zyxel	Nebula Nr7101 Firmware	All	All	All	All
Hardware	Zyxel	Nr7101	-	All	All	All
Operating System	Zyxel	Nr7101 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Access denied Zyxel Networks	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.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](#)