



CVE-2023-41352

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-41352
State	PUBLIC
Assigner	cve@cert.org.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 06:15:00 UTC
Updated	2023-11-13 19:31:00 UTC
Description	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of insufficient filtering for user input. A remote attacker with administrative access can exploit this vulnerability to execute arbitrary code on the affected device. The vulnerability is caused by insufficient filtering of user input in the device's web interface. The vulnerability is present in the device's web interface, which is accessible to anyone with access to the device's IP address. The vulnerability is present in the device's web interface, which is accessible to anyone with access to the device's IP address.

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nokia	G-040w-q	-	All	All	All
Operating System	Nokia	G-040w-q Firmware	g040wqr201207	All	All	All

References

Reference

- TWCERT/CC台灣電腦網路危機處理暨協調中心|企業資安通報協處|資安情資分享|漏洞通報|資安聯盟|資安電子報-中華電信 NOKIA G-040W-Q - 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](#).

Free CVE JSON API cve.report/api

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