



CVE-2023-39240

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

Summary

CVE	CVE-2023-39240
State	PUBLIC
Assigner	cve@cert.org.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-07 08:15:00 UTC
Updated	2024-03-27 07:15:00 UTC
Description	It is identified a format string vulnerability in ASUS RT-AX56U V2's iperf client function API. This vulnerability is caused by I

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Asus	Rt-ac86u	-	All	All	All
Operating System	Asus	Rt-ac86u Firmware	3.0.0.4_386_51529	All	All	All
Hardware	Asus	Rt-ax55	-	All	All	All
Operating System	Asus	Rt-ax55 Firmware	3.0.0.4.386_50460	All	All	All
Hardware	Asus	Rt-ax56u V2	-	All	All	All
Operating System	Asus	Rt-ax56u V2 Firmware	3.0.0.4.386_50460	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-ASUS RT-AX55、RT-AX56U](#)

[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](#)