



CVE-2023-40072

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

Summary

CVE	CVE-2023-40072
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-18 10:15:00 UTC
Updated	2024-01-23 10:15:00 UTC
Description	OS command injection vulnerability in WAB-S600-PS all versions, and WAB-S300 all versions allows an authenticated user

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Elecom	Wab-s300	-	All	All	All
Operating System	Elecom	Wab-s300 Firmware	All	All	All	All
Hardware	Elecom	Wab-s600-ps	-	All	All	All
Operating System	Elecom	Wab-s600-ps Firmware	All	All	All	All

References

Reference	Source
www.elecom.co.jp/news/security/20230810-01	M
無線LANルーター・中継器のセキュリティ向上のためのファームウェアアップデート・対策実施のお願い エレコム株式会社 ELECOM	
JVNVU#91630351: Multiple vulnerabilities in ELECOM and LOGITEC network devices	M
CVE Program record	C
NVD vulnerability detail	N

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](#)