CVE-2026-24465

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-24465
State	PUBLISHED
Assigner	jpcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-03 07:16:13 UTC
Updated	2026-04-14 12:59:18 UTC
Description	Stack-based buffer overflow vulnerability exists in ELECOM wireless LAN access point devices. A crafted packet may lead

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from vultures@jpcert.or.jp

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000190000 probability, percentile 0.049800000 (date 2026-04-15)

Problem Types: CWE-121 | CWE-121 Stack-based buffer overflow

Version	Source	Type	Score	Severity	Vector
4.0	vultures@jpcert.or.jp	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.0	vultures@jpcert.or.jp	Secondary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	CNA	CVSS	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Elecom	Wab-s300iw-ac	All	All	All	All
Operating System	Elecom	Wab-s300iw-ac Firmware	All	All	All	All
Hardware	Elecom	Wab-s300iw-pd	All	All	All	All
Operating System	Elecom	Wab-s300iw-pd Firmware	All	All	All	All

Hardware	Elecom	Wab-s300iw2-pd	All	All	All	All
Operating System	Elecom	Wab-s300iw2-pd Firmware	All	All	All	All
Hardware	Elecom	Wab-s733iw-ac	All	All	All	All
Operating System	Elecom	Wab-s733iw-ac Firmware	All	All	All	All
Hardware	Elecom	Wab-s733iw-pd	All	All	All	All
Operating System	Elecom	Wab-s733iw-pd Firmware	All	All	All	All
Hardware	Elecom	Wab-s733iw2-pd	All	All	All	All
Operating System	Elecom	Wab-s733iw2-pd Firmware	All	All	All	All
Hardware	Elecom	Wrc-x1500gs-b	All	All	All	All
Operating System	Elecom	Wrc-x1500gs-b Firmware	All	All	All	All
Hardware	Elecom	Wrc-x1500gsa-b	All	All	All	All
Operating System	Elecom	Wrc-x1500gsa-b Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ELECOM CO.LTD.	WAB-S733IW2-PD	affected v5.5.00 and earlier versions	Not specified
CNA	ELECOM CO.LTD.	WAB-S733IW-AC	affected v5.5.00 and earlier versions	Not specified
CNA	ELECOM CO.LTD.	WAB-S733IW-PD	affected all versions	Not specified
CNA	ELECOM CO.LTD.	WAB-S300IW2-PD	affected v5.5.00 and earlier versions	Not specified
CNA	ELECOM CO.LTD.	WAB-S300IW-AC	affected v5.5.00 and earlier versions	Not specified
CNA	ELECOM CO.LTD.	WAB-S300IW-PD	affected all versions	Not specified

References

Reference	Source	Link	Tags
jvn.jp/en/jp/JVN94012927	vultures@jpcert.or.jp	jvn.jp	Third Party Advisory
www.elecom.co.jp/news/security/20260203-01	vultures@jpcert.or.jp	www.elecom.co.jp	Vendor Advisory
www.elecom.co.jp/news/security/20260203-02	vultures@jpcert.or.jp	www.elecom.co.jp	Vendor Advisory
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.

Free CVE JSON API cve.report/api

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