Carlson Software VASCO-B GNSS Receiver Missing Authentication for Critical Function

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

Summary

CVE	CVE-2026-3893
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 19:37:39 UTC
Updated	2026-04-28 20:10:23 UTC
Description	The Carlson VASCO-B GNSS Receiver lacks an authentication mechanism, allowing an attacker with network access to di

Risk And Classification

Primary CVSS: v3.1 9.4 CRITICAL from ics-cert@hq.dhs.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Problem Types: CWE-306 | CWE-306 CWE-306

Version	Source	Type	Score	Severity	Vector
3.1	ics-cert@hq.dhs.gov	Secondary	9.4	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H
3.1	CNA	CVSS	9.4	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
Low

Integrity
High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Carlson Software	VASCO-B GNSS Receiver	affected 1.4.0 custom	Not specified
CNA	Carlson Software	VASCO-B GNSS Receiver	unaffected 1.4.0	Not specified

References

Reference	Source	Link	Tags
www.carlsonsw.com/support-and-training	ics-cert@hq.dhs.gov	www.carlsonsw.com	
www.cve.org/CVERecord	ics-cert@hq.dhs.gov	www.cve.org	
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-11...	ics-cert@hq.dhs.gov	github.com	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

Vendor Comments And Credit

Discovery Credit

CNA: Souvik Kandar reported this vulnerability to CISA. (en)

Additional Advisory Data

Solutions

CNA: Carlson Software recommends users update to Version 1.4.0 or greater. For more information contact Carlson Software https://www.carlsonsw.com/support-and-training/

There are currently no legacy QID mappings associated with this CVE.