Copeland XWEB and XWEB Pro Stack-based Buffer Overflow

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

Summary

CVE	CVE-2026-20797
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-27 02:16:18 UTC
Updated	2026-05-10 14:16:46 UTC
Description	A stack based buffer overflow exists in an API route of XWEB Pro version 1.12.1 and prior, enabling unauthenticated attack

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.000270000 probability, percentile 0.076900000 (date 2026-05-12)

Problem Types: CWE-787 | CWE-121 | WE-121 | CWE-121 CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ics-cert@hq.dhs.gov	Secondary	4.3	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/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	Copeland	Xweb 300d Pro	-	All	All	All
Operating System	Copeland	Xweb 300d Pro Firmware	All	All	All	All
Hardware	Copeland	Xweb 500b Pro	-	All	All	All
Operating System	Copeland	Xweb 500b Pro Firmware	All	All	All	All
Hardware	Copeland	Xweb 500d Pro	-	All	All	All
Operating System	Copeland	Xweb 500d Pro Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Copeland	Copeland XWEB 300D PRO	affected 1.12.1 custom	Not specified
CNA	Copeland	Copeland XWEB 500D PRO	affected 1.12.1 custom	Not specified
CNA	Copeland	Copeland XWEB 500B PRO	affected 1.12.1 custom	Not specified

References

Reference	Source	Link	Tags
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-05...	ics-cert@hq.dhs.gov	github.com	Third Party
www.cisa.gov/news-events/ics-advisories/icsa-26-057-10	ics-cert@hq.dhs.gov	www.cisa.gov	Third Party
webapps.copeland.com/Dixell/Pages/SystemSoftwareUpdate	ics-cert@hq.dhs.gov	webapps.copeland.com	Product
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: Amir Zaltzman and Noam Moshe of Claroty Team82 reported this vulnerability to CISA.

(en)

Additional Advisory Data

Additional Advisory Data

Solutions

CNA: Copeland has provided a fix for the vulnerabilities and recommends users update the XWEB Pro to the latest version by going to their software update page https://webapps.copeland.com/Dixell/Pages/SystemSoftwareUpdate in the sections dedicated to the different XWEBPRO models page.

CNA: Alternatively, a user logged into an XWEB Pro with internet access can update XWEB Pro directly from Copeland servers via the menu SYSTEM -- Updates | Network.

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