v2board / Xboard Authentication Token Exposure via loginWithMailLink

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

Summary

CVE	CVE-2026-39912
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 19:16:25 UTC
Updated	2026-04-09 19:16:25 UTC
Description	V2Board 1.6.1 through 1.7.4 and Xboard through 0.1.9 expose authentication tokens in HTTP response bodies of the loginV

Risk And Classification

Primary CVSS: v4.0 9.1 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/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

Problem Types: CWE-201 | CWE-201 CWE-201 Insertion of Sensitive Information Into Sent Data

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.1	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	9.1	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S
3.1	disclosure@vulncheck.com	Primary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/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 v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	V2board	V2board	affected 1.6.1 1.7.4 semver
CNA	V2board	V2board	affected bdb10bed32c5f37df2f0872c3cb354e9b7a293bd 0ca47622a50116d0ddd7ffb316b157afb57d25e8
CNA	Cedar2025	Xboard	affected 0.1.9 semver

CNA	Cedar2025	Xboard	unaffected 121511523f04882ec0c7447acd9b8ebcb8a47957 git

References

Reference	Source	Link
github.com/v2board/v2board/blob/0ca47622a50116d0ddd7ffb316b157afb57d25e8...	disclosure@vulncheck.com	github.com
github.com/v2board/v2board/pull/981	disclosure@vulncheck.com	github.com
github.com/cedar2025/Xboard/commit/121511523f04882ec0c7447acd9b8ebcb8a47957	disclosure@vulncheck.com	github.com
github.com/cedar2025/Xboard/blob/1fe6531924cc1ec662a88b9ef725afcf78d660b...	disclosure@vulncheck.com	github.com
chocapikk.com/posts/2026/xboard-v2board-account-takeover	disclosure@vulncheck.com	chocapikk.com
www.vulncheck.com/advisories/v2board-xboard-authentication-token-exposure-via-l...	disclosure@vulncheck.com	www.vulncheck.com
github.com/cedar2025/Xboard/blob/1fe6531924cc1ec662a88b9ef725afcf78d660b...	disclosure@vulncheck.com	github.com
github.com/cedar2025/Xboard/pull/873	disclosure@vulncheck.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Valentin Lobstein (Chocapikk) (en)

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