Domoticz < 2026.1 Stored XSS via Hardware Configuration Endpoint

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

Summary

CVE	CVE-2026-1001
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 19:16:30 UTC
Updated	2026-04-01 15:42:23 UTC
Description	Domoticz versions prior to 2026.1 contain a stored cross-site scripting vulnerability in the Add Hardware and rename device

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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: 0.000440000 probability, percentile 0.136440000 (date 2026-04-05)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

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

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Domoticz	Domoticz	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

Source	Vendor	Product	Version	Platforms
CNA	Domoticz	Domoticz	affected 2026.1 semver	Not specified

References

Reference	Source	Link
www.domoticz.com/2026.1	disclosure@vulncheck.com	www.domoticz.com
www.vulncheck.com/advisories/domoticz-stored-xss-via-hardware-configuration-end...	disclosure@vulncheck.com	www.vulncheck.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Kacper Leszczyński (en)

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