



Stored XSS vulnerability in Host navigator widget maintenance tooltip

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-23926
State	PUBLISHED
Assigner	Zabbix
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 08:16:01 UTC
Updated	2026-05-06 08:16:01 UTC
Description	An authenticated (non-super) administrator can create a maintenance period with a JavaScript payload that is executed by

Risk And Classification

Primary CVSS: v4.0 7.3 HIGH from security@zabbix.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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

Version	Source	Type	Score	Severity	Vector
4.0	security@zabbix.com	Secondary	7.3	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X
4.0	CNA	CVSS	7.3	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

High

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Zabbix	Zabbix	affected 7.0.0 7.0.23 git	Not specified
CNA	Zabbix	Zabbix	affected 7.4.0 7.4.7 git	Not specified

References

Reference	Source	Link	Tags
support.zabbix.com/browse/ZBX-27758	security@zabbix.com	support.zabbix.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Zabbix wants to thank Daniel Santos (@bananabr) for submitting this report on the HackerOne bug bounty platform. (en)

Additional Advisory Data

Solutions

CNA: Update the affected components to their respective fixed versions.

Workarounds

CNA: Disable the Host navigator widget via Administration -> General -> Modules.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)