



# Stored XSS vulnerability in the Item history/Plain text widget

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

## Summary

<b>CVE</b>	CVE-2026-23928
<b>State</b>	PUBLISHED
<b>Assigner</b>	Zabbix
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 08:16:03 UTC
<b>Updated</b>	2026-05-06 08:16:03 UTC
<b>Description</b>	The Item history widget (in Zabbix 7.0+) or the Plain text widget (in Zabbix 6.0) can execute injected JavaScript when HTML

## 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	<a href="#">Zabbix</a>	<a href="#">Zabbix</a>	affected 6.0.0 6.0.44 git	Not specified
CNA	<a href="#">Zabbix</a>	<a href="#">Zabbix</a>	affected 7.0.0 7.0.23 git	Not specified
CNA	<a href="#">Zabbix</a>	<a href="#">Zabbix</a>	affected 7.4.0 7.4.7 git	Not specified

### References

Reference	Source	Link	Tags
<a href="https://support.zabbix.com/browse/ZBX-27760">support.zabbix.com/browse/ZBX-27760</a>	<a href="mailto:security@zabbix.com">security@zabbix.com</a>	<a href="https://support.zabbix.com">support.zabbix.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

#### Solutions

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

#### Workarounds

**CNA:** Do not use HTML display in Item history/Plain text widget or disable this widget entirely in Administration -> General -> Modules (Zabbix 7.0+).

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](#)