مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Stored Cross-Site Scripting (XSS) Vulnerabilities in Zabbix Frontend Components

Tracking #:432318905

Date:06-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two high-severity stored cross-site scripting (XSS) vulnerabilities have been identified in the frontend components of Zabbix, tracked as CVE-2026-23926 and CVE-2026-23928.

TECHNICAL DETAILS:

Two high-severity stored cross-site scripting (XSS) vulnerabilities have been identified in the frontend components of Zabbix, tracked as CVE-2026-23926 and CVE-2026-23928. These flaws allow attackers to inject malicious JavaScript that is persistently stored and executed in the context of other users' sessions.

1. **CVE-2026-23926 – Stored XSS in Host Navigator Widget**
   - **Component:** Frontend (Host Navigator widget – Maintenance tooltip)
   - **Vulnerability Type:** Stored Cross-Site Scripting (XSS)
   - **CVSS Score:** 7.3 (High)
   - **Attack Vector:** Network
   - **Privileges Required:** High (authenticated non-super administrator)
   - **User Interaction:** Required

Vulnerability Overview:

- An authenticated administrator can inject **malicious JavaScript payloads** into a maintenance period.
- The payload is stored and later executed when another user opens or hovers over the **maintenance tooltip** in the Host Navigator widget.

Exploitation Flow:

- Attacker creates a maintenance entry containing malicious script
- Victim user accesses Host Navigator widget
- Tooltip renders and executes embedded JavaScript

Impact:

- Execution of arbitrary JavaScript in victim's browser
- Session hijacking and credential theft
- Unauthorized actions via victim's privileges

Affected Versions:

- 7.0.0 – 7.0.23
- 7.4.0 – 7.4.7

Fixed Versions:

- 7.0.24
- 7.4.8

2. **CVE-2026-23928 – Stored XSS in Item History / Plain Text Widget**
   - **Component:** Frontend (Item History widget / Plain Text widget)
   - **Vulnerability Type:** Stored Cross-Site Scripting (XSS)
   - **CVSS Score:** 7.3 (High)
   - **Attack Vector:** Network
   - **Privileges Required:** High (via controlled monitored host)
   - **User Interaction:** Required

Vulnerability Overview:

- Malicious JavaScript can be injected through monitoring data originating from a compromised or attacker-controlled host.
- When dashboards render this data with HTML display enabled, the payload executes in the user's browser.

Exploitation Flow:

- Attacker controls monitored host
- Sends crafted payload in item data
- Dashboard loads Item History / Plain Text widget
- Payload executes when viewed

Impact:

- Persistent XSS across dashboards
- Broader attack surface affecting multiple users
- Potential lateral movement and privilege escalation

Affected Versions:

- 6.0.0 – 6.0.44
- 7.0.0 – 7.0.23
- 7.4.0 – 7.4.7

Fixed Versions:

- 6.0.45
- 7.0.24
- 7.4.8

RECOMMENDATIONS:

- Upgrade to patched versions for the affected components.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.zabbix.com/browse/ZBX-27760
- https://support.zabbix.com/browse/ZBX-27758