مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple High-Severity Vulnerabilities in Zabbix

Tracking #:432318699

Date:01-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Zabbix affecting its Server, Proxy, and API components. These issues could allow authenticated users to access sensitive data, bypass validation controls, execute arbitrary commands, and perform SQL injection, potentially leading to system compromise.

TECHNICAL DETAILS:

Vulnerability Details
High-Severity Vulnerabilities:
CVE-2026-23919

- Insufficient isolation of JavaScript execution contexts may allow non-super administrators to access sensitive data across hosts.

CVE-2026-23920

- Improper regex validation can be bypassed using newline injection, potentially leading to command injection.

CVE-2026-23921

- Blind SQL injection in the API (sortfield parameter) may allow data exfiltration and account compromise.

Affected Products

- Zabbix Server, Proxy, API

Affected Versions:

- 6.0.0 – 6.0.40
- 7.0.0 – 7.0.21
- 7.2.0 – 7.2.14
- 7.4.0 – 7.4.5

Fixed Versions

- **CVE-2026-23919:** Fixed in 6.0.41, 7.0.19, 7.2.13, 7.4.3
- **CVE-2026-23920 & CVE-2026-23921:** Fixed in 7.0.22, 7.2.15, 7.4.6

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Zabbix.

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-27638
- https://support.zabbix.com/browse/ZBX-27639
- https://support.zabbix.com/browse/ZBX-27640