



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical SQL Injection Vulnerability in Zabbix

Tracking #:432316578

Date:29-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical SQL injection vulnerability has been discovered in Zabbix, a widely-used open-source IT infrastructure monitoring tool.

TECHNICAL DETAILS:

A critical SQL injection vulnerability (CVE-2024-42327) has been discovered in Zabbix, a widely-used open-source IT infrastructure monitoring tool. This vulnerability, with a CVSS score of 9.9, allows attackers to escalate privileges, potentially gaining full control over Zabbix instances.

Vulnerability Details:

- CVE ID: CVE-2024-42327
- Severity: **Critical** (CVSS 9.9)
- Vulnerable Product: Zabbix
- Affected Versions: All versions prior to 6.0.32rc1, 6.4.17rc1, and 7.0.1rc1
- Vulnerability Type: SQL Injection
- Affected Endpoint: user.get API
- Exploitation Risk: High – Non-admin users with API access (including those with the default "User" role) can exploit this vulnerability to execute arbitrary SQL code.

Fixed Version:

- Zabbix 6.0.32rc1 (or later)
- Zabbix 6.4.17rc1 (or later)
- Zabbix 7.0.1rc1 (or later)

RECOMMENDATIONS:

Ensure that all Zabbix deployments are updated to the latest versions.

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-25623>