مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical RCE Vulnerability in Zabbix

Tracking #:432316144

Date:14-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability, has been discovered in the Zabbix monitoring solution, which could lead to a full system compromise.

TECHNICAL DETAILS:

Zabbix, a widely-adopted open-source solution for enterprise-level IT infrastructure monitoring, has disclosed a critical security vulnerability that could lead to full system compromise.

Vulnerability Overview:

- **CVE Identifier:** CVE-2024-22116
- **CVSS Score:** 9.9 (Critical)
- **Type:** Remote Code Execution (RCE)
- **Description:** Vulnerability exists in the script execution functionality within the Monitoring Hosts section, specifically in the Ping script. It allows an administrator with restricted permissions to execute arbitrary code due to a lack of default escaping for script parameters.
- **Impact:** Allows attackers to execute arbitrary code on the server, potentially leading to full system compromise.

Affected Versions:

- 6.4.0 to 6.4.15
- 7.0.0alpha1 to 7.0.0rc2

Fixed Versions:

- 6.4.16rc1
- 7.0.0rc3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update affected version to fixed version as soon as possible to mitigate the risk of exploitation.

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://www.zabbix.com/security_advisories#ZBV-2024-08-09-2