Security Advisory 2024-082

Zabbix Server Critical Arbitrary Code Execution Vulnerability

August 16, 2024 — v1.0

TLP:CLEAR

History:

- *16/08/2024 — v1.0 – Initial publication*

Summary

On August 13, 2024, a critical vulnerability, **CVE-2024-22116**, was disclosed in Zabbix Server, allowing attackers with restricted administrative permissions to execute arbitrary code. The flaw, identified in the Ping script execution within the Monitoring Hosts section, can compromise the entire infrastructure. The vulnerability carries a CVSS score of 9.9 [1].

Technical Details

CVE-2024-22116 is a code injection vulnerability (CWE-94) where improper control over script parameters allows arbitrary code execution via the Ping script in the Monitoring Hosts section [1].

Affected Products

- Zabbix Server versions 6.4.0 to 6.4.15
- Zabbix Server versions 7.0.0alpha1 to 7.0.0rc2

Recommendations

CERT-EU strongly recommends upgrading to Zabbix versions 6.4.16rc1 or 7.0.0rc3 immediately, as no workarounds are available.

References

[1] https://cybersecuritynews.com/zabbix-server-vulnerability/