Hive Pro

THREAT ADVISORY

Zabbix affected by two actively exploited vulnerabilities

TA2022041

Threat Level RED

Publish Date – Feb 23, 2022

Multiple security vulnerabilities have been discovered in Zabbix (open-source network traffic monitoring software) Web Frontend component while implementing client-side sessions storage and are being actively exploited as per CISA. Successful exploitation of these vulnerabilities may allow an attacker to bypass authentication, escalate privileges and execute an arbitrary code on a targeted server instance that could lead to the complete compromise of the network infrastructure.

An authentication bypass is one of the vulnerabilities, which has been assigned CVE-2022-23131. This issue occurs since the Zabbix Web Frontend is automatically configured with a highly-privileged user named "Admin" which may allow attackers to gain admin privileges to the Zabbix Frontend. SAML authentication must be enabled for the attack to be successful, and the actor must know the Zabbix user's name (or use the guest account, which is disabled by default).

Another one is an improper access control vulnerability that has been issued CVE-2022-23134. This issue exists due to unsafe use of the session in the "setup.php" file which is usually run by system administrators when first deploying Zabbix Web Frontend and later access is only allowed to authenticated and highly-privileged users. Attackers can override the existing configuration files and gain access to the dashboard with a highly-privileged account.

These vulnerabilities are actively being exploited and hence organizations should apply the patch as soon as possible.

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
T1190: Exploit Public-Facing Application
TA0004: Privilege Escalation
T1068: Exploitation for Privilege Escalation
TA0002: Execution
T1059: Command and Scripting Interpreter

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-23131	Zabbix version 5.4.0 to 5.4.8, 6.0alpha1	cpe:2.3:a:zabbix:zabbix:*:*:*:*:*:*:*:*	Zabbix Frontend Authentication Bypass Vulnerability	CWE-290
CVE-2022-23134	Zabbix version 5.4.0 to 5.4.8 6.0.0 to 6.0.0beta1	cpe:2.3:a:zabbix:zabbix:*:*:*:*:*:*:*:*	Zabbix Frontend Improper Access Control Vulnerability	CWE-863

Patch Link

https://support.zabbix.com/browse/ZBX-20384
https://support.zabbix.com/browse/ZBX-20350

References

https://blog.sonarsource.com/zabbix-case-study-of-unsafe-session-storage
https://www.cisa.gov/uscert/ncas/current-activity/2022/02/22/cisa-adds-two-known-exploited-vulnerabilities-catalog