

CVE-2022-23131

Zabbix Frontend Authentication Bypass Vulnerability

Exigent

CISA KEV since Feb 22, 2022

Actively exploited

In the case of instances where the SAML SSO authentication is enabled (non-default), session data can be modified by a malicious actor, because a user login stored in the session was not verified. Malicious unauthenticated actor may exploit this issue to escalate privileges and gain admin access to Zabbix Frontend. To perform the attack, SAML authentication is required to be enabled and the actor has to know the username of Zabbix user (or use the guest account, which is disabled by default).

EVRS 86 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.957 99.87th percentile · FIRST	CISA DEADLINE Mar 8, 2022 KEV since 2022 · listed over a year
--	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.957 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
zabbix	$\geq 5.4.0 \leq 5.4.8$ 6.0.0	after 5.4.8	NVD

Sources

Vendor guidance	support.zabbix.com/browse/ZBX-20350	NVD	nvd.nist.gov/vuln/detail/CVE-2022-23131
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-28222
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-23131		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.