Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0320

Kwetsbaarheden verholpen in Zabbix

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 20-08-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Zabbix SIA heeft meerdere kwetsbaarheden verholpen in Zabbix, inclusief de API, Frontend, script item en preprocessing componenten, en de Windows Agent installer.

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van Zabbix.

- Een probleem in het login lockout mechanisme zorgt ervoor dat meerdere gelijktijdige mislukte inlogpogingen niet correct worden geteld, waardoor een aanvaller de lockout kan omzeilen en meer wachtwoordpogingen kan doen dan bedoeld.
- In de OAuth-configuratie voor e-mailmedia kan een Super Admin via aanpassingen aan de 'Token endpoint' het client secret onthullen en wijzigen.
- Prototype pollution in de searchParamsToObject() functie leidt tot persistente cross-site scripting (XSS) via onveilige URL-parameterverwerking en jQuery elementcreatie.
- De Frontend webserver bevat een actie (popup.testtriggerexpr) die door niet-geauthenticeerde gebruikers kan worden misbruikt om een denial of service (DoS) te veroorzaken door overmatige CPU-belasting.
- Geauthenticeerde gebruikers kunnen via de validate.api.exists actie plaintext user macro waarden uitlezen, wat gevoelige informatie blootlegt. In Zabbix 7.4 is een cryptografische sleutel voor het ondertekenen van Frontend sessies onjuist opgeslagen in de database seed, waardoor sessiecookies kunnen worden vervalst bij gebruik van SAML authenticatie en gastgebruikers. De validate.api.exists actie kan ook leiden tot DoS door excessief CPU-gebruik bij speciaal samengestelde verzoeken.
- In de script item en preprocessing JavaScript HttpRequest logica kan een administrator geheugen buiten de bedoelde grenzen uitlezen, wat kan leiden tot informatielekken.
- De API host.get actie maakt het mogelijk voor geauthenticeerde gebruikers om de pre-shared key (PSK) van een host te achterhalen, wat de vertrouwelijkheid en integriteit van gegevens ondermijnt.
- Een authenticeerde administrator kan via speciaal samengestelde JavaScript scripts in preprocessing of script items een DoS veroorzaken door server- of proxycrashes, specifiek in community packages voor Fedora en EPEL.
- De Windows Agent installer detecteert nu onveilige installatiepaden die kwetsbaar zijn voor DLL sideloading en vraagt expliciete bevestiging van de gebruiker voordat de installatie doorgaat.

Oplossingen

Zabbix SIA heeft updates uitgebracht om deze kwetsbaarheden in Zabbix te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.zabbix.com/browse/ZBX-28067
- https://support.zabbix.com/browse/ZBX-28068
- https://support.zabbix.com/browse/ZBX-28069
- https://support.zabbix.com/browse/ZBX-28070
- https://support.zabbix.com/browse/ZBX-28071
- https://support.zabbix.com/browse/ZBX-28072
- https://support.zabbix.com/browse/ZBX-28073
- https://support.zabbix.com/browse/ZBX-28074
- https://support.zabbix.com/browse/ZBX-28075
- https://support.zabbix.com/browse/ZBX-28076
- https://support.zabbix.com/browse/ZBX-28077

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-1199	6.9 MEDIUM
CVE-2026-23922	2.1 LOW
CVE-2026-23929	8.5 HIGH
CVE-2026-23930	5.3 MEDIUM
CVE-2026-23931	5.3 MEDIUM
CVE-2026-23933	7.7 HIGH
CVE-2026-23934	5.1 MEDIUM
CVE-2026-23935	6.8 MEDIUM
CVE-2026-23937	6.0 MEDIUM
CVE-2026-23938	2.1 LOW
CVE-2026-59781	5.4 MEDIUM

CWE's

CWE	Beschrijving
CWE-125	Out-of-bounds Read
CWE-203	Observable Discrepancy
CWE-248	Uncaught Exception
CWE-259	Use of Hard-coded Password
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-405	Asymmetric Resource Consumption (Amplification)
CWE-427	Uncontrolled Search Path Element
CWE-522	Insufficiently Protected Credentials
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Getroffen producten

Zabbix
Zabbix

Disclaimer