Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0462

Kwetsbaarheden verholpen in Zabbix

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 02-12-2024

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 heeft kwetsbaarheden verholpen in de Zabbix server en frontend.

Duiding

De kwetsbaarheden omvatten een stack buffer overflow in de zbx_snmp_cache_handle_engineid functie, die kan leiden tot het uitvoeren van willekeurige code of een denial of service. Daarnaast is er een SQL-injectie kwetsbaarheid die niet-beheerders met API-toegang in staat stelt om ongeautoriseerde toegang tot gevoelige gegevens te verkrijgen. Ook zijn er kwetsbaarheden gerapporteerd die kunnen leiden tot gegevensvervalsing in de gebruikersinterface en een kleine geheugenlek die gevoelige informatie kan blootstellen.

Oplossingen

Zabbix heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://support.zabbix.com/browse/ZBX-25621
- https://support.zabbix.com/browse/ZBX-25622
- https://support.zabbix.com/browse/ZBX-25623
- https://support.zabbix.com/browse/ZBX-25624
- https://support.zabbix.com/browse/ZBX-25625
- https://support.zabbix.com/browse/ZBX-25626
- https://support.zabbix.com/browse/ZBX-25630
- https://support.zabbix.com/browse/ZBX-25635

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-36464	2.7 LOW
CVE-2024-36466	8.8 HIGH
CVE-2024-36468	3.0 LOW
CVE-2024-42326	

CVE-2024-42327	9.9 CRITICAL
CVE-2024-42328	3.3 LOW
CVE-2024-42329	3.3 LOW
CVE-2024-42330	9.1 CRITICAL
CVE-2024-42331	3.3 LOW
CVE-2024-42332	3.7 LOW
CVE-2024-42333	2.7 LOW

CWE's

CWE	Beschrijving
CWE-690	Unchecked Return Value to NULL Pointer Dereference
CWE-126	Buffer Over-read
CWE-134	Use of Externally-Controlled Format String
CWE-256	Plaintext Storage of a Password
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-121	Stack-based Buffer Overflow
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

zabbix
frontend

zabbix

Disclaimer