



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

Getroffen producten

zabbix
frontend

zabbix

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.