



NCSC-2026-0396

Kwetsbaarheden aangetroffen in Zammad

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 30-09-2026

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

Er zijn twee zeroday-kwetsbaarheden aangetroffen in Zammad.

Duiding

De eerste kwetsbaarheid heeft het kenmerk CVE-2026-102489 toegekend gekregen. De kwetsbaarheid stelt een ongeauthenticeerde kwaadwillende op afstand in staat om willekeurige code uit te voeren. De kwetsbaarheid is aanwezig in Zammad versies 6.3.0 tot en met 6.5.4.

De tweede kwetsbaarheid heeft het kenmerk CVE-2026-102490 toegekend gekregen. Deze kwetsbaarheid stelt een kwaadwillende die over lage rechten beschikt in staat om rootrechten te verkrijgen op het kwetsbare systeem. Deze kwetsbaarheid is aanwezig in alle gangbare versies van Zammad.

De kwetsbaarheden worden in ieder geval sinds 21 september 2026 actief misbruikt voor het op afstand verkrijgen van rootrechten op het systeem waar Zammad op draait.

Oplossingen

Zammad heeft beveiligingsupdates uitgebracht voor het verhelpen van CVE-2026-102489. Het NCSC adviseert om de updates met spoed te installeren. Stel applicatie- en netwerklogs veilig alvorens je deze updates installeert. Dergelijke loggegevens kunnen in een later stadium nodig zijn om vast te stellen of jouw Zammad-omgeving in de zeroday-fase is gecompromitteerd.

De tweede kwetsbaarheid is vooralsnog niet verholpen. Neem contact op met je leverancier als je vragen over deze kwetsbaarheid hebt.

Referenties

➤ <https://csirt.divd.nl/DIVD-2026-00015>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-102489	9.4 CRITICAL
➤ CVE-2026-102490	9.4 CRITICAL

CWE's

CWE	Beschrijving
CWE-280	Improper Handling of Insufficient Permissions or Privileges

Getroffen producten

Zammad GmbH
Zammad

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.