



NCSC-2025-0272

Kwetsbaarheid verholpen in FreePBX

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 29-08-2025

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

FreePBX heeft een kwetsbaarheid verholpen in versies 15, 16 en 17.

Duiding

De kwetsbaarheid stelt aanvallers in staat om ongeautoriseerde toegang te krijgen en mogelijk op afstand code uit te voeren, door misbruik te maken van een validatie- en saneringfout in de verwerking van door gebruikers aangeleverde invoer, zoals in de "endpoint" module.

FreePBX meldt dat actief misbruik heeft plaatsgevonden op meerdere systemen met FreePBX versie 16 en 17 die voorzien waren van onvoldoende IP-filtering en ACLs en waarbij het managementinterface rechtstreeks verbonden was met het internet.

Oplossingen

- FreePBX heeft updates uitgebracht om de kwetsbaarheid te verhelpen en geeft het advies om te bevestigen dat de geïnstalleerde "endpoint" module voldoet aan de minimaal gepatchte versies.
- Systemen die niet automatisch updaten, of gebruikers die handmatig willen bijwerken, kunnen dit doen via het Administrator Control Panel menu.
- Het NCSC adviseert de update zo spoedig mogelijk te installeren en je systeem te controleren op aanwezigheid IOC's wanneer je je managementinterface naar het internet hebt ontsloten.
- Ontsluiten van de managementinterface aan het internet is alleen aan te raden in gevallen waarin dit noodzakelijk is. In die gevallen is het advies om deze slechts bereikbaar te maken vanaf specifieke IP adressen en eventueel met gebruik van een VPN.
- Meer informatie, waaronder beschikbare IOC's, zijn te vinden op de website van FreePBX. Deze is als referentie aan dit beveiligingsadvies toegevoegd.

Referenties

- <https://community.freepbx.org/t/security-advisory-please-lock-down-your-administrator-access/107203>
- <https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-57819	10.0 CRITICAL

CWE's

CWE	Beschrijving
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CWE-288	Authentication Bypass Using an Alternate Path or Channel

Getroffen producten

FreePBX
security-reporting

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.