



NCSC-2025-0299

Kwetsbaarheden verholpen in Zenitel ICX500 en ICX510 Gateway

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 26-09-2025

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

Zenitel heeft kwetsbaarheden verholpen in de ICX500 en ICX510 Gateway producten.

Duiding

De kwetsbaarheden stellen kwaadwillenden in staat om ongeautoriseerde toegang te krijgen tot de Billing Admin endpoint en om willekeurige commando's uit te voeren op het apparaat. Dit kan leiden tot ernstige compromittering van de beschikbaarheid, vertrouwelijkheid en integriteit van de apparaten. De kwetsbaarheid met kenmerk CVE-2025-59816 in de Billing Admin stelt aanvallers in staat om directe queries uit te voeren tegen de Billing Admin database, waardoor ze toegang krijgen tot alle opgeslagen gegevens, inclusief platte tekst gebruikersreferenties.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de lokale infrastructuur. Het is goed gebruik dergelijke infrastructuur niet publiek toegankelijk te hebben.

Oplossingen

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

Referenties

➤ https://wiki.zenitel.com/wiki/ICX_1.4.3.X_-_Release_Notes

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-59814	8.8 HIGH
➤ CVE-2025-59815	8.4 HIGH
➤ CVE-2025-59816	7.3 HIGH
➤ CVE-2025-59817	8.4 HIGH

CWE's

CWE	Beschrijving
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

Zenitel
ICX500
ICX510
TCIS-3+

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.