



# NCSC-2025-0121

## Kwetsbaarheid verholpen in Gladinet CentreStack

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-04-2025

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Gladinet heeft een kwetsbaarheid verholpen in CentreStack (Versies tot 16.1.10296.56315).

## Duiding

De kwetsbaarheid bevindt zich in de manier waarop hardcoded machineKeys en cryptografische sleutels worden gebruikt, hetgeen resulteert in een ernstige deserialisatiekwetsbaarheid. De kwetsbaarheid maakt het voor een kwaadwillende mogelijk om malafide ViewState-payloads te genereren die door het getroffen systeem als geldig worden geaccepteerd. Hierdoor kan willekeurige code op afstand worden uitgevoerd binnen de context van het kwetsbare systeem. Gladinet geeft aan dat de kwetsbaarheid sinds maart 2025 actief wordt misbruikt. Ook het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) meldt via de Known Exploited Vulnerability Database dat de kwetsbaarheid is misbruikt.

## Oplossingen

Gladinet heeft een beveiligingsupdate uitgebracht in versie 16.4.10315.56368 van CentreStack. In deze versie wordt tijdens de installatie automatisch een unieke machineKey gegenereerd, waarmee de onderliggende kwetsbaarheid wordt gemitigeerd. Het Nationaal Cyber Security Centrum (NCSC) adviseert organisaties met klem om hun systemen zo spoedig mogelijk bij te werken naar deze versie. Indien een directe update niet haalbaar is, wordt aanbevolen om handmatig een unieke machineKey te genereren en toe te passen. Aangezien de kwetsbaarheid actief is misbruikt, adviseert het NCSC organisaties tevens om nader technisch onderzoek uit te voeren. Raadpleeg de bijgevoegde referenties voor aanvullende toelichting en technische details.

## Referenties

- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://nvd.nist.gov/vuln/detail/CVE-2025-30406>
- <https://gladinetsupport.s3.us-east-1.amazonaws.com/gladinet/securityadvisory-cve-2005.pdf>

## Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-30406	6.3 MEDIUM

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-321</a>	Use of Hard-coded Cryptographic Key

## Getroffen producten

<b>Gladinet</b>
CentreStack

## 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.