Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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
CWE-321	Use of Hard-coded Cryptographic Key

Getroffen producten

Gladinet
CentreStack

Disclaimer