



NCSC-2025-0009

Kwetsbaarheid verholpen in FortiNet FortiOS en FortiProxy

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 28-01-2025

Revisie: 1.0.1

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

Update Revisie 1

Er is PoC verschenen waarmee misbruik van deze kwetsbaarheid is aangetoond.

Feiten

FortiNet heeft een kwetsbaarheid verholpen in FortiOS en FortiProxy.

Duiding

De kwetsbaarheid bevindt zich in de node.js implementatie van de management-webinterface en stelt een kwaadwillende in staat om authenticatie te omzeilen om zo zonder voorafgaande authenticatie of autorisaties super-admin te worden op het kwetsbare systeem.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de management-webinterface. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheer-omgeving.

FortiNet meldt dat actief misbruik is waargenomen op FortiGate systemen waarop de kwetsbare FortiOS of FortiProxt draait. Ook hebben onderzoekers Proof-of-Concept-Code (PoC) gepubliceerd, waarmee de kwetsbaarheid kan worden aangetoond.

FortiNet heeft Indicators of Compromise (IoC's) vrijgegeven, waarmee mogelijke compromittatie kan worden ontdekt:

- Following login activity log with random scrip and dstip:

```
type="event" subtype="system" level="information" vd="root" logdesc="Admin login successful"
sn="1733486785" user="admin" ui="jsconsole" method="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1
action="login" status="success" reason="none" profile="super_admin" msg="Administrator admin
logged in successfully from jsconsole"
```

- Following admin creation log with seemingly randomly generated user name and source IP:

```
type="event" subtype="system" level="information" vd="root" logdesc="Object attribute configured"
user="admin" ui="jsconsole(127.0.0.1)" action="Add" cfgtid=1411317760 cfgpath="system.admin"
cfgobj="v0cep" cfgattr="password[*]accprofile[super_admin]vdom[root]" msg="Add system.admin
v0cep"
```

Oplossingen

FortiNet heeft updates en handelingsperspectieven uitgebracht om de kwetsbaarheid te verhelpen en eventuele compromittatie te onderzoeken. Tevens adviseert FortiNet expliciet om toegang tot de management-webinterface te blokkeren of zoveel als mogelijk te beperken middels 'local-in policies'. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.fortiguard.com/psirt/FG-IR-24-535>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-55591	

CWE's

CWE	Beschrijving
➤ CWE-288	Authentication Bypass Using an Alternate Path or Channel

Getroffen producten

fortinet
fortios
fortiproxy

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.