



# NCSC-2026-0060

## Kwetsbaarheden verholpen in Fortinet FortiSandbox, FortiAuthenticator en FortiClient

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-02-2026

### **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

Fortinet heeft kwetsbaarheden verholpen in FortiSandbox (versies 4.4.8 en 5.0.5), FortiAuthenticator (versies 6.3 tot 6.6.6) en FortiClient (versies 7.0, 7.2 en 7.4).

## Duiding

De kwetsbaarheid in FortiSandbox betreft Cross-site Scripting, waardoor niet-geauthenticeerde aanvallers willekeurige commando's kunnen uitvoeren via speciaal gemaakte verzoeken. De kwetsbaarheid in FortiAuthenticator betreft een ontbrekende autorisatie die het mogelijk maakt voor alleen-lezen gebruikers om lokale gebruikersaccounts te wijzigen via een onbeveiligd bestand upload endpoint. De kwetsbaarheid in FortiClient stelt lokale aanvallers met lage privileges in staat om willekeurige bestandswijzigingen uit te voeren met verhoogde rechten door middel van speciaal gemaakte named pipe berichten, wat ongeautoriseerde toegang tot systeem bestanden mogelijk maakt.

## Oplossingen

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

## Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-25-093>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-528>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-661>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-52436</a>	8.8 HIGH
➤ <a href="#">CVE-2026-21743</a>	7.2 HIGH
➤ <a href="#">CVE-2025-62676</a>	7.1 HIGH

## CWE's

CWE	Beschrijving
> <a href="#">CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> <a href="#">CWE-862</a>	Missing Authorization
> <a href="#">CWE-59</a>	Improper Link Resolution Before File Access ('Link Following')

## Getroffen producten

Fortinet
FortiAuthenticator
FortiClient
FortiClientWindows
FortiSandbox

## 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.