Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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
CVE-2025-52436	8.8 HIGH
CVE-2026-21743	7.2 HIGH
CVE-2025-62676	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-862	Missing Authorization
CWE-59	Improper Link Resolution Before File Access ('Link Following')

Getroffen producten

Fortinet
FortiAuthenticator
FortiClient
FortiClientWindows
FortiSandbox

Disclaimer