



NCSC-2025-0386

Kwetsbaarheden verholpen in Fortinet producten

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 28-01-2026

Revisie: 1.0.3

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 3

Onderzoekers melden actief misbruik waar te nemen van de kwetsbaarheden met kenmerk CVE-2025-59718 en CVE-2025-59719 en hebben IoC's gedeeld.

Feiten

Fortinet heeft kwetsbaarheden verholpen in FortiOS, FortiProxy, FortiWeb en FortiSwitchManager.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om toegang te krijgen tot de systemen door gebruik te maken van verschillende technieken, waaronder het omzeilen van FortiCloud SSO-login authenticatie via speciaal vervaardigde SAML-berichten, het behouden van actieve SSLVPN-sessies ondanks een wachtwoordwijziging, en het uitvoeren van ongeautoriseerde operaties via vervalste HTTP- of HTTPS-verzoeken. Dit kan leiden tot ongeautoriseerde toegang tot gevoelige API-gegevens en andere netwerkbronnen.

update 16-12-25: Onderzoekers melden actief misbruik waar te nemen van de kwetsbaarheden met kenmerk CVE-2025-59718 en CVE-59719. Deze kwetsbaarheden stellen kwaadwillenden in staat om de Single Sign On te omzeilen en zo toegang te krijgen tot de kwetsbare systemen. De onderzoekers hebben Indicators of Compromise (IoC's) gepubliceerd om misbruik te kunnen onderzoeken. Het NCSC adviseert zo spoedig mogelijk de updates van Fortinet in te zetten, indien dit nog niet is gedaan, eventueel de mitigerende maatregelen in te zetten en middels de gepubliceerde IoC's te onderzoeken of misbruik heeft plaatsgevonden en op basis daarvan de administrator accounts het password van te roteren. Het NCSC adviseert aanvullend om te overwegen de open sessies van administrators te sluiten na inzet van de updates.

Zie voor detailinformatie van de IoC's: <https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-ssso-logins-following-disclosure-cve-2025-59718-cve-2025-59719/>

update 23-01-26: De updates werken niet voldoende om te beschermen tegen de FortiCloud single sign-on (SSO) bypass kwetsbaarheden (CVE-2025-59718 en CVE-2025-59719). Er is misbruik van deze kwetsbaarheden waargenomen op systemen die de laatste updates hadden doorgevoerd. Zowel Fortinet als ArcticWolf hebben IoC's en mitigerende maatregelen ter beschikking gesteld.

update 28-01-26: Bron CERT-AT bijgevoegd, bevat nieuwe IoC's voor onderzoek.

Zie voor detailinformatie van de IoC's en mitigerende maatregelen: <https://www.fortinet.com/blog/psirt-blogs/analysis-of-ssso-abuse-on-fortios> & <https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-configuration-changes-fortinet-fortigate-devices-via-ssso-accounts/>

Oplossingen

Als mitigerende maatregel tegen de authenticatie-bypass kan FortiCloud SSO login worden uitgeschakeld. Fortinet heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-configuration-changes-fortinet-fortigate-devices-via-sso-accounts/>
- <https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-sso-logins-following-disclosure-cve-2025-59718-cve-2025-59719/>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-268>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-411>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-647>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-945>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-984>
- <https://www.cert.at/en/blog/2026/1/look-at-forticloud-sso-bypass-exploitation>
- <https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-59718	9.8 CRITICAL
➤ CVE-2025-59719	9.8 CRITICAL
➤ CVE-2025-62631	5.6 MEDIUM
➤ CVE-2024-47570	6.6 MEDIUM
➤ CVE-2025-64471	4.9 MEDIUM
➤ CVE-2025-64447	8.1 HIGH

CWE's

CWE	Beschrijving

➤ CWE-347	Improper Verification of Cryptographic Signature
➤ CWE-532	Insertion of Sensitive Information into Log File
➤ CWE-613	Insufficient Session Expiration

Getroffen producten

Fortinet
FortiOS
FortiProxy
FortiSwitchManager
FortiWeb

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.