Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0240

Kwetsbaarheden verholpen in meerdere Fortinet producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-07-2026

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 meerdere versies van FortiSIEM (Windows Agent en algemene productversies), FortiOS, FortiPAM en FortiProxy.

Duiding

Een kwetsbaarheid in FortiSIEM Windows Agent (versies 7.4.0 tot en met 7.4.1) met kenmerk CVE-2026-59841 stelt kwaadwillenden op hetzelfde lokale netwerk in staat om privileges te verhogen wanneer de functie 'Supers Override' actief is. Hierdoor kunnen kwaadwillenden willekeurige code uitvoeren en de integriteit van de agent compromitteren.

De overige kwetsbaarheden zijn door een geauthenticeerde aanvaller met verhoogde privileges op afstand, of met fysieke toegang, te misbruiken. Zie bijgevoegde referenties voor meer informatie.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheden in FortiSIEM, FortiOS, FortiPAM en FortiProxy te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-26-155
- https://www.fortiguard.com/psirt/FG-IR-26-149
- https://www.fortiguard.com/psirt/FG-IR-26-150
- https://www.fortiguard.com/psirt/FG-IR-26-151

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-59841	7.5 HIGH
CVE-2026-59839	5.5 MEDIUM
CVE-2026-23573	6.1 MEDIUM
CVE-2026-59838	5.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints

Getroffen producten

Fortinet
FortiOS
FortiPAM
FortiProxy
FortiSIEM
FortiSIEMWindowsAgent

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.