Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0041

Kwetsbaarheid verholpen in Fortinet producten

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 28-01-2026

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 een kwetsbaarheid verholpen in FortiAnalyzer, FortiManager, FortiOS en FortiProxy producten.

Duiding

De kwetsbaarheid bevindt zich in specifieke implementaties van FortiCloud SSO-authenticatie. De kwetsbaarheid stelt aanvallers met een geregistreerd apparaat en een FortiCloud-account in staat om de authenticatie te omzeilen en toegang te krijgen tot andere geregistreerde apparaten wanneer FortiCloud SSO-authenticatie is ingeschakeld.

Fortinet heeft aangegeven dat er actief misbruik van de kwetsbaarheid is waargenomen. Fortinet heeft in hun advisory ook indicators-of-compromise (IoC's) beschikbaar gesteld om misbruik van de kwetsbaarheid te onderkennen. Het NCSC adviseert partijen die gebruikmaken van de kwetsbare implementaties om ook middels deze IoC’s terug te kijken in de logging.

Oplossingen

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

Referenties

- https://www.fortiguard.com/psirt/FG-IR-26-060
- https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-24858	9.8 CRITICAL

CWE's

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

Getroffen producten

Fortinet
FortiAnalyzer
FortiManager
FortiOS
FortiProxy

Disclaimer