



Advisory NCSC-2026-0428

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Fortinet FortiSandbox

Publicatiedatum: 14-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Fortinet heeft kwetsbaarheden verholpen in FortiSandbox.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-107656 heeft een CVSS-score van 9,6 en betreft een authenticatieomzeiling in de webmanagementinterface van FortiSandbox. Een niet-geauthenticeerde kwaadwillende kan via speciaal vervaardigde HTTP-verzoeken de authenticatie omzeilen en ongeautoriseerd code of commando's uitvoeren.

De kwetsbaarheden met kenmerk CVE-2026-106172 en CVE-2026-106170 zijn beide als middelmatig ingeschaald. CVE-2026-106172 betreft het gebruik van een hardcoded cryptografische sleutel in de Fabric API, waardoor een niet-geauthenticeerde kwaadwillende mogelijk verhoogde toegangsrechten kan verkrijgen. CVE-2026-106170 betreft een niet-afgevangen uitzondering (exception) en kan door een kwaadwillende met verhoogde rechten worden misbruikt om de werking van de GUI en CLI blijvend te verstoren.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Voor FortiSandbox PaaS gelden overeenkomstige update- of migratie-instructies. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-26-176>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-179>
- <https://www.fortiguard.com/psirt/FG-IR-26-185>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-107656	9.8 CRITICAL
CVE-2026-106170	4.9 MEDIUM
CVE-2026-106172	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-248	Uncaught Exception
CWE-321	Use of Hard-coded Cryptographic Key

Getroffen producten

Fortinet
FortiSandbox
FortiSandbox Cloud

fortinet
FortiSandbox PaaS

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 or 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.