



NCSC-2026-0121

Kwetsbaarheden verholpen in Fortinet FortiSandbox

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-04-2026

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 meerdere kwetsbaarheden verholpen in FortiSandbox, waaronder in on-premises versies en FortiSandbox Cloud, waarvan twee door Fortinet als kritiek zijn beoordeeld.

Duiding

Een kwaadwillende kan de kwetsbaarheden met kenmerk CVE-2026-39813 en CVE-2026-39808 misbruiken doordat in FortiSandbox sprake is van OS command injection en een path traversal-kwetsbaarheid in de JRPC API. Hierdoor kan een niet-geauthenticeerde aanvaller via gemanipuleerde HTTP-verzoeken ongeautoriseerde code of commando's uitvoeren en authenticatie omzeilen.

De overige kwetsbaarheden omvatten een path traversal-kwetsbaarheid waardoor een geprivilegieerde super-admin met CLI-toegang via HTTP-verzoeken mappen kan verwijderen, en meerdere cross-site scripting kwetsbaarheden (reflected en stored) waardoor via gemanipuleerde HTTP-verzoeken XSS-aanvallen kunnen worden uitgevoerd.

Oplossingen

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

Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-26-109>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-110>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-112>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-115>
- <https://www.fortiguard.com/psirt/FG-IR-26-100>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-25691	6.7 MEDIUM
➤ CVE-2026-39812	4.8 MEDIUM
➤ CVE-2025-61886	5.4 MEDIUM

> CVE-2026-39813	9.8 CRITICAL
> CVE-2026-39808	9.8 CRITICAL

CWE's

CWE	Beschrijving
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-24	Path Traversal: '../filedir'
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

Fortinet
FortiSandbox
FortiSandbox Cloud
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 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.