



NCSC-2025-0083

Kwetsbaarheden verholpen in Fortinet FortiSandbox

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-03-2025

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 FortiSandbox.

Duiding

De kwetsbaarheid met kenmerk CVE-2024-45328 omvat een onjuiste autorisatie die het mogelijk maakt voor laaggeprivilegieerde beheerders om verhoogde CLI-commando's uit te voeren via de GUI-console.

Daarnaast is er een SQL-injectie kwetsbaarheid met kenmerk CVE-2024-54026 die door geprivilegieerde aanvallers kunnen worden misbruikt om ongeautoriseerde commando's uit te voeren.

Er is ook kwetsbaarheid met kenmerk CVE-2024-54027 met een probleem in een hardcoded cryptografische sleutel, dat het mogelijk maakt voor super-beheerders om gevoelige gegevens te lezen via de CLI.

De kwetsbaarheden met kenmerken CVE-2024-52960, CVE-2024-52961 en CVE-2024-54018 stellen een geauthenticeerde aanvaller met alleen-lezen rechten in staat, ongeautoriseerde commando's uit te voeren door speciaal samengestelde verzoeken te verzenden. Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang en controle over de getroffen systemen.

Oplossingen

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

Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-24-261>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-353>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-306>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-305>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-110>

Kwetsbaarheden

| CVE | CVSS Score |
|------------------|------------|
| ➤ CVE-2024-45328 | 8.5 HIGH |
| ➤ CVE-2024-54026 | 5.3 MEDIUM |

| | |
|------------------|------------|
| > CVE-2024-54027 | 8.4 HIGH |
| > CVE-2024-52961 | 8.7 HIGH |
| > CVE-2024-54018 | 8.6 HIGH |
| > CVE-2024-52960 | 5.3 MEDIUM |

CWE's

| CWE | Beschrijving |
|-----------|--|
| > CVE-863 | Incorrect Authorization |
| > CVE-89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| > CVE-321 | Use of Hard-coded Cryptographic Key |
| > CVE-78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| > CVE-602 | Client-Side Enforcement of Server-Side Security |

Getroffen producten

| |
|-----------------|
| Fortinet |
| FortiSandbox |

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.