Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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

Getroffen producten

Fortinet
FortiSandbox

Disclaimer