Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0287

Kwetsbaarheden verholpen in Fortinet

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-07-2024

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 aantal kwetsbaarheden verholpen in FortiAIOps, Fortinet FortiPortal, FortiWeb en Fortinet FortiExtender.

Duiding

De meest serieuze kwetsbaarheden zijn CVE-2024-23663, CVE-2024-27782 en CVE-2024-27784. Welke in Fortinet FortiExtender en FortiAIOps zitten.

Fortinet FortiExtender: Fortinet ForiExtender is een apparaat welke internet verbinding via 4g en 5g ondersteund. Een kwaadwillende kan de CVE-2024-23663 kwetsbaarheid die in Fortinet FortiExtender misbruiken om via HTTP verzoeken verhoogde rechten te krijgen.

FortiAIOps (versie 2.0.0): De andere twee kwetsbaarheden, CVE-2024-27784 en CVE-2024-27782, zitten in FortiAIOps versie 2.0.0. FortiAIOps is een platform welke netwerk verkeer ondersteund door artificiële intelligentie en machine learning. Dit doet dit door diverse data stromen van het netwerk te integreren. Een kwaadwillende kan de CVE-2024-27782 kwetsbaarheid misbruiken om met gestolen sessie tokens ongeautoriseerde verzoeken in te dienen. Een kwaadwillende kan de CVE-2024-27784 kwetsbaarheid misbruiken, mits hij geauthenticeerd is tot FortiAIOps, om gevoelige data in te zien van een API endpoint of log files.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-22-326
- https://fortiguard.fortinet.com/psirt/FG-IR-23-459
- https://fortiguard.fortinet.com/psirt/FG-IR-24-011
- https://fortiguard.fortinet.com/psirt/FG-IR-24-069
- https://fortiguard.fortinet.com/psirt/FG-IR-24-072
- https://fortiguard.fortinet.com/psirt/FG-IR-24-073
- https://fortiguard.com/psirt/FG-IR-23-459
- https://fortiguard.fortinet.com/psirt/FG-IR-22-326
- https://fortiguard.fortinet.com/psirt/FG-IR-24-011
- https://fortiguard.fortinet.com/psirt/FG-IR-24-069
- https://fortiguard.fortinet.com/psirt/FG-IR-24-072
- https://fortiguard.fortinet.com/psirt/FG-IR-24-073

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-21759	4.3 MEDIUM
CVE-2024-33509	4.8 MEDIUM
CVE-2024-27782	8.1 HIGH
CVE-2024-27784	8.8 HIGH
CVE-2024-23663	8.8 HIGH
CVE-2024-27785	5.4 MEDIUM

CWE's

CWE	Beschrijving
CWE-1236	Improper Neutralization of Formula Elements in a CSV File
CWE-284	Improper Access Control
CWE-295	Improper Certificate Validation
CWE-532	Insertion of Sensitive Information into Log File
CWE-613	Insufficient Session Expiration
CWE-639	Authorization Bypass Through User-Controlled Key

Getroffen producten

fortinet
fortiaiops
fortiextender
fortiportal
fortiweb

Disclaimer