Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0423

Kwetsbaarheid ontdekt in Fortinet FortiManager

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 23-10-2024

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 kwetsbaarheid verholpen in FortiGuard.

Duiding

Er is, voor de bekendmaking van de CVE en patch, misbruik van CVE-2024-47575 waargenomen. Er bestaat daarmee een risico op misbruik van deze CVE voordat de beschikbare patch is geïnstalleerd. Het NCSC adviseert om, naast het patchen van uw FortiManager met de beschikbaar gestelde patch, onderzoek te doen aan de hand van beschikbare Indicators of Compromise (IoC's) om mogelijk misbruik te onderkennen. Een kwaadwillende kan toegang hebben gehad tot uw FortiGuard/FortiManager omgeving door een ander Fortinet serienummer in uw FortiGuard te registreren. Via het certificaat zou de kwaadwillende de authenticatie hebben kunnen omzeilen. Het NCSC doet onderzoek naar deze kwetsbaarheid en stelt eventuele nieuwe IoC's beschikbaar.

```
De onderstaande IoC's kunnen u ondersteunen bij forensisch onderzoek:
Fortinet serienummers:
FMG-VMTM23017412
FMG-VM0000000000
Netwerk IoC's:
45.32.41.202
104.238.141.143
158.247.199.3
```

De aanval stelt een kwaadwillende instaat om configuratie gegevens op te halen van uw firewall/netwerk omgeving. Ook stelt dit een kwaadwillende in staat om (VPN) account credentials en certificaten in te zien, welke de mogelijkheid geven om via bestaande accounts uw netwerk te betreden. Mocht u indicatoren zien van misbruik, adviseert het NCSC daarom ook om accounts te resetten en certificaten te vernieuwen. Wat precies in een aanval gestolen zou kunnen zijn ligt echter aan de geïmplementeerde configuratie en kan per casus verschillen.

Oplossingen

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

Referenties

- https://www.cve.org/CVERecord?id=CVE-2024-47575
- https://fortiguard.fortinet.com/psirt/FG-IR-24-423

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-47575	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-306	Missing Authentication for Critical Function

Getroffen producten

fortinet
fortimanager

Disclaimer