L.s.,

Wij zijn stichting Z-CERT, het Computer Emergency Response Team voor de Nederlandse zorgsector. Bij deze willen wij u informeren over een belangrijke cybersecurity aangelegenheid.

Er bevindt zich een ernstigste kwetsbaarheid in de VPN-SSL zoals in gebruik bij FortiGate, in de producten FortiGate, FortiProxy en Fortiweb. Dit stelt een ongeauthenticeerde kwaadwillende op afstand in staat om willekeurige code uit te voeren op het kwetsbare systeem en mogelijk het systeem over te nemen. Deze kwetsbaarheid heeft kenmerk CVE-2023-27997 toegekend gekregen.

Er zijn verschillende signalen dat er (op korte termijn) misbruik wordt gemaakt van deze kwetsbaarheid [1][2].

Mogelijke oplossingen:
Fortinet heeft updates uitgebracht die onder andere deze kwetsbaarheid in FortiOS verhelpt, zoals gebruikt in FortiGate, FortiProxy en FortiWeb. Zie:

https://www.fortiguard.com/psirt/FG-IR-23-125
https://www.fortiguard.com/psirt/FG-IR-23-119
https://www.fortiguard.com/psirt/FG-IR-23-111
https://www.fortiguard.com/psirt/FG-IR-22-380
https://www.fortiguard.com/psirt/FG-IR-22-393
https://www.fortiguard.com/psirt/FG-IR-23-095
https://www.fortiguard.com/psirt/FG-IR-22-463
https://www.fortiguard.com/psirt/FG-IR-22-494
https://www.fortiguard.com/psirt/FG-IR-22-375
https://www.fortiguard.com/psirt/FG-IR-22-468
https://www.fortiguard.com/psirt/FG-IR-22-455

Voor een beveiligingsadvies betreffende de kwetsbaarheid met kenmerk CVE-2023-27997 heeft Fortinet een kennisitem ter beschikking gesteld [3]. U kunt ook terecht bij het advies dat het Nationaal Cyber Security Centre van Nederland (het NCSC-NL) op haar website heeft gepubliceerd [4].

Z-CERT adviseert om de kwetsbaarheid zo spoedig mogelijk te patchen, als dat nog niet is gebeurd. Indien patchen op korte termijn niet lukt, is het aan te raden om het systeem tijdelijk offline te halen tot patchen wel lukt.

[1] https://www.cisa.gov/news-events/alerts/2023/06/13/cisa-adds-one-known-exploited-vulnerability-catalog
[2] https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign
[3] https://www.fortiguard.com/psirt/FG-IR-23-097
[4] https://www.ncsc.nl/actueel/advisory?id=NCSC-2023-0282

Met vriendelijke groet,

Team Z-CERT
Sectorale CERT voor de zorg
Stationsplein 121 | 3818 LE | Amersfoort T +31 (0)33 737 0609 | www.Z-CERT.nl