Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0357

Kwetsbaarheden verholpen in Zyxel Flex en USG Firewalls

2024-09-03 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Zyxel heeft kwetsbaarheden verholpen in de firmware van ATP en USG Flex firewalls.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, mogelijk ongeathenticeerd een beperkte set commando's uit te voeren op het kwetsbare systeem, of middels een Cross-Site-Scripting-aanval willekeurige code uit te voeren in de browser van het slachtoffer. Het is niet uit te sluiten, dat wanneer het slachtoffer verhoogde rechten heeft op het kwetsbare systeem, de kwaadwillende hiermee de mogelijkheid krijgt om met de rechten van een administrator commando's uit te voeren op het kwetsbare systeem.

Oplossingen

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

Referenties

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-09-03-2024