Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0357

Kwetsbaarheden verholpen in Zyxel Flex en USG Firewalls

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 03-09-2024

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

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

Duiding

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

Kwetsbaarheden

CVE	CVSS Score
› CVE-2024-6343	4.9 MEDIUM
› CVE-2024-7203	7.2 HIGH
› CVE-2024-42057	8.1 HIGH
› CVE-2024-42058	7.5 HIGH
› CVE-2024-42059	7.2 HIGH
› CVE-2024-42060	7.2 HIGH
› CVE-2024-42061	6.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-476	NULL Pointer Dereference
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

zyxel
atp_series_firmware
usg_flex_50_w__series_firmware
usg_flex_series_firmware
usg20_w_-vpn_series_firmware

Disclaimer