



Advisory NCSC-2024-0356

Kwetsbaarheid verholpen in Zyxel Access Points en Secure Routers

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.first.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 een kwetsbaarheid verholpen in diverse types Access Points en Secure Routers.

Interpretaties

De kwetsbaarheid bevindt zich in de wijze waarop het cgi-systeem de parameter 'host' verwerkt en stelt een kwaadwillende in staat om op OS-niveau commando's uit te voeren.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de cgi-interface. Het is goed gebruik om een dergelijke interface niet publiek toegankelijk te hebben.

Oplossingen

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

Referenties

- <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024>