Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0468

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in Zyxel product

Publicatiedatum: 05-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Zyxel heeft een kwetsbaarheid verholpen in de firmware van de Zyxel GS1900-24E netwerk switch, specifiek in versie 2.90(AAHK.2)C0 en eerder.

Duiding

De kwetsbaarheid betreft een out-of-bounds write in het CGI-programma van de management-interface van het apparaat. Een niet-geauthenticeerde aanvaller met toegang tot de management-interface kan via speciaal vervaardigde HTTP-verzoeken commando's uitvoeren op het systeem. De fout ontstaat door onjuiste bounds checking in de CGI-component, wat kan leiden tot het uitvoeren van commando's. Volgens openbare nieuwsberichten zou de kwetsbaarheid actief als zero-day zijn misbruikt. Het NCSC heeft dit nog niet onafhankelijk kunnen verifiëren.

Het is goed gebruik om managementinterfaces in een apart netwerk onder te brengen en deze niet rechtstreeks vanaf het internet bereikbaar te maken.

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-out-of-bounds-write-vulnerability-in-gs1900-series-switches-11-03-2026

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-107441	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-787	Out-of-bounds Write

Getroffen producten

ZyXEL
GS1900-48 firmware
GS1900-8 firmware
GS1900-8HP firmware

Zyxel
GS1900 Series Switches
GS1900-10HP firmware
GS1900-16 firmware
GS1900-24 firmware
GS1900-24E firmware
GS1900-24EP firmware
GS1900-48HPv2 firmware
GS1900-HPv2 firmware

zyxel
gs1900_series_switches

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.