Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0469

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in OpenSSH door OpenSSH Project

Publicatiedatum: 06-11-2026

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

Het OpenSSH project heeft een kwetsbaarheid verholpen in sshd van OpenSSH versies ouder dan 10.6p2. De kwetsbaarheid treft Linux systemen die gebruikmaken van musl libc en waarop PAM niet wordt gebruikt.

Duiding

De kwetsbaarheid betreft een bypass van de SSH-wachtwoordauthenticatie bij gebruik van wachtwoorden met een lengte van 257 tot 1024 bytes. De oorzaak ligt in de interactie tussen de authenticatieafhandeling van OpenSSH (sshd) en de implementatie van crypt() in musl libc, in omgevingen waarin PAM niet wordt gebruikt. Hierdoor kan een aanvaller onder specifieke omstandigheden de wachtwoordverificatie omzeilen en mogelijk ongeautoriseerde toegang tot het systeem verkrijgen.

Misbruik vereist dat aan meerdere voorwaarden wordt voldaan:

- Het systeem draait Linux met musl libc, zoals Alpine Linux.
- OpenSSH draait zonder PAM.
- PasswordAuthentication is ingeschakeld.
- Er is een account aanwezig met een * als password hash en minimaal één ander account met een geldige SHA-256 of SHA-512 password hash.

De kwetsbaarheid is daarmee beperkt tot specifieke configuraties. Reguliere Debian en Ubuntu installaties, die gebruikmaken van glibc, vallen buiten het beschreven toepassingsgebied.

Vanuit securityoogpunt wordt geadviseerd SSH-beheerdiensten niet rechtstreeks aan het internet bloot te stellen. Beperk de toegang waar mogelijk tot vertrouwde netwerken en schakel wachtwoordauthenticatie uit wanneer deze niet noodzakelijk is.

Oplossingen

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

Referenties

- https://www.openssh.org/releasenotes.html#10.6p2

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-123158	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-394	Unexpected Status Code or Return Value

Getroffen producten

OpenBSD
OpenSSH

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.