Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0210

Kwetsbaarheden verholpen in libssh2 door libssh

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 23-06-2026

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

libssh heeft kwetsbaarheden verholpen in libssh2 tot en met versie 1.11.1.

Duiding

De eerste kwetsbaarheid betreft een pre-authenticatie denial of service in de SSH_MSG_EXT_INFO handler. Een kwaadaardige SSH-server kan een speciaal geconstrueerde extension_count waarde sturen, waardoor de client in een CPU-uitputtingslus terechtkomt en de verwerking van SSH-berichten verstoord wordt. De tweede kwetsbaarheid zit in de ssh2_transport_read() functie, waar onjuiste bounds checking op de packet_length variabele leidt tot een out-of-bounds write. Dit kan door een aanvaller worden misbruikt om met speciaal geconstrueerde SSH-pakketten een Denial-of-Service te veroorzaken, of in theorie om willekeurige code uit te voeren op het getroffen systeem, indien er geen additionele maatregelen zijn genomen als Address Space Layout Randomization (ALSR). Dit is echter geen gebruikelijke instelling op systemen. Beide kwetsbaarheden zijn aanwezig in alle implementaties die libssh2 versie 1.11.1 of lager gebruiken.

Oplossingen

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

Referenties

- https://github.com/advisories/GHSA-3CFQ-4XX4-RMPG
- https://github.com/advisories/GHSA-R8MH-X5QV-7GG2

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-55199	8.2 HIGH
CVE-2026-55200	9.2 CRITICAL

CWE's

CWE	Beschrijving
CWE-680	Integer Overflow to Buffer Overflow

CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

Getroffen producten

Open Source
libssh2
libssh2
libssh2

Disclaimer