Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0033

Kwetsbaarheid verholpen in GNU Inetutils telnetd

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 21-01-2026

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

Beveiligingsonderzoekers hebben een een kwetsbaarheid aangetroffen in Inetutils telnetd (versie 2.7). Deze kwetsbaarheid is volgens de onderzoekers al aanwezig sinds versie 1.9.3 die uit is gekomen in 2015.

Duiding

De kwetsbaarheid bevindt zich in de manier waarop de telnetd-service omgaat met de USER-omgeving variabele. Door deze variabele in te stellen op '-f root', kunnen kwaadwillenden authenticatie omzeilen en rootrechten bemachtigen. Dit is een ernstig risico voor de systeemintegriteit.

Deze kwetsbaarheid is zeer eenvoudig uit te buiten en exploitcode hiervoor is publiek beschikbaar. Het NCSC verwacht dan ook dat er bij publiek toegankelijke telnet servers op korte termijn misbruik van deze kwetsbaarheid plaats zal vinden.

Oplossingen

Het NCSC adviseert om managementinterfaces zoals Telnet niet aan het internet te koppelen, maar enkel op aparte managementnetwerken beschikbaar te stellen. Dit beperkt het aanvalsoppervlak aanzienlijk. Daarnaast adviseert het NCSC om IP-allowlisting toe te passen en de Telnet-interface enkel voor vertrouwde clients beschikbaar te stellen.

Er zijn patches beschikbaar om de kwetsbaarheid te verhelpen. Deze moeten echter in de packages van de diverse distributies verwerkt worden voordat ze door te voeren zijn. Tot die tijd zijn de patches slechts door te voeren door deze handigmatig in de code (in telnetd/utility.c) aan te passen en vervolgens zelfstandig te compileren.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://codeberg.org/inetutils/inetutils/commit/ccba9f748aa8d50a38d7748e2e60362edd6a32cc
- https://codeberg.org/inetutils/inetutils/commit/fd702c02497b2f398e739e3119bed0b23dd7aa7b
- https://seclists.org/oss-sec/2026/q1/89
- https://www.gnu.org/software/inetutils/

Kwetsbaarheden

CVE	CVSS Score

CVE-2026-24061	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')

Getroffen producten

GNU
InetUtils

Disclaimer