



Advisory NCSC-2026-0461

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Linux kernel

Publicatiedatum: 30-10-2026

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 delen. 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

Linux heeft kwetsbaarheden verholpen in de IPv4 TCP stack en het IPv4 networking subsystem van de Linux kernel.

Duiding

De eerste kwetsbaarheid betreft een race condition in de IPv4 TCP stack die leidt tot een use-after-free van socketopties tijdens gelijktijdige TCP SYN retransmissies of request socket migraties. Dit kan resulteren in systeeminstabiliteit of geheugenbeschadiging. De oorzaak is het voortijdig vrijgeven van inet_opt en ireq_opt structuren.

De tweede kwetsbaarheid betreft een onjuiste validatie van checksum metadata in IPv4 pakketten, waardoor lokale aanvallers of onbetrouwbare gast-virtuele machines malformed checksum data kunnen gebruiken om willekeurige code op de host uit te voeren, systeemcrashes te veroorzaken of gevoelige informatie te lekken. Deze kwetsbaarheid, bekend als PwnEscape, maakt gast-naar-host ontsnapping mogelijk.

Hoewel door de complexiteit van misbruik en binnen de bekende distro's aanwezige aanvullende maatregelen, grootschalig misbruik niet waarschijnlijk is, zijn deze kwetsbaarheden in de linux-kernel toch opvallend, aangezien kwetsbaarheden in de netwerkstacks van de kernel een van de weinige soorten kwetsbaarheden zijn die op afstand en zonder voorafgaande authenticatie zijn te misbruiken, maar wel potentieel de kernel in gevaar brengen.

Oplossingen

De ontwikkelaars van Linux hebben updates uitgebracht die de kwetsbaarheden verhelpen. De grote Linux distributie vendors nemen deze updates op in de huidige kernels. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://git.kernel.org/pub/scm/linux/security/vulns.git/plain/cve/published/2026/CVE-2026-98432.mbox>
- <https://git.kernel.org/pub/scm/linux/security/vulns.git/plain/cve/published/2026/CVE-2026-99999.mbox>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-98432	9.8 CRITICAL
CVE-2026-99999	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-787	Out-of-bounds Write
CWE-825	Expired Pointer Dereference

Getroffen producten

Debian
linux

Linux
Linux

Microsoft
azl3 kernel 6.6.157.1-1 on Azure Linux 3.0

NetApp

Linux kernel

Nutanix

Nutanix AHV

Oracle

Oracle Linux

RESF

RESF Rocky Linux

Red Hat

Red Hat Enterprise Linux

SUSE

SUSE openSUSE

SuSE Linux

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 or 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.