



NCSC-2026-0131

Kwetsbaarheid verholpen in Linux kernel cryptographic subsystem

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 01-05-2026

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

De Linux kernel heeft een kwetsbaarheid verholpen in de algif_aead crypto module binnen het cryptographic subsystem.

Duiding

De kwetsbaarheid bevindt zich in de algif_aead crypto module van de Linux kernel, waar een fout in de in-place operatie optrad wanneer bron- en bestemmingsmappings verschilden. Hiermee is het mogelijk om voor een gebruiker zonder sudo rechten verhoogde privileges te verkrijgen.

Oplossingen

De kernelontwikkelaars hebben de algif_aead-module teruggezet naar een out-of-place-operatie, waarmee de problematische in-place-verwerking is verwijderd. Daarnaast is de complexiteit verminderd door data direct te kopiëren, in plaats van te vertrouwen op de foutgevoelige in-place-methode. Zie de bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.cve.org/CVERecord?id=CVE-2026-31431>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-31431	7.8 HIGH

CWE's

CWE	Beschrijving
➤ CWE-669	Incorrect Resource Transfer Between Spheres
➤ CWE-1288	Improper Validation of Consistency within Input

Getroffen producten

Debian
linux
Linux
Linux
Linux Kernel
Microsoft
azl3 kernel 6.6.130.1-3 on Azure Linux 3.0
azl3 kernel 6.6.134.1-2 on Azure Linux 3.0
Open Source
Open Source Linux Kernel
Red Hat
Red Hat Enterprise Linux
Red Hat Enterprise Linux 10
Red Hat Enterprise Linux 6
Red Hat Enterprise Linux 7
Red Hat Enterprise Linux 8
Red Hat Enterprise Linux 9

kernel
kernel- rt

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.