Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0464

PRIORITEIT: NORMAAL

# Kwetsbaarheid verholpen in LXD van Canonical

Publicatiedatum: 02-11-2026

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

Canonical heeft een kwetsbaarheid verholpen in LXD.

# Duiding

De kwetsbaarheid (CVE-2026-112816) wordt veroorzaakt door onjuiste validatie van certificaatketens binnen de HTTPS API van Canonical LXD. De kwetsbaarheid treft LXD-versies vóór 4.0.15, 5.0.11, 5.21.9 en 6.10.1 binnen de betreffende releasebranches.

Hierdoor kunnen niet-geauthenticeerde aanvallers die netwerktoegang hebben tot de HTTPS API en beschikken over het publieke certificaat van een vertrouwde client, zich voordoen als die client. Dit is mogelijk doordat LXD ten onrechte alle certificaten in de aangeboden certificaatketen controleert tegen de trust store, terwijl alleen het leaf-certificaat cryptografisch aan het bezit van de bijbehorende private key is gekoppeld.

Succesvolle exploitatie kan leiden tot ongeautoriseerde toegang tot de LXD-cluster en de beheerde virtuele machines, met privileges gelijk aan die van de geïmiteerde client. Wanneer deze client over voldoende beheerdersrechten beschikt, kan dit uiteindelijk leiden tot root-toegang op de onderliggende host.

De kwetsbaarheid heeft een CVSS 4.0-score van 10.0 (Critical) en treft meerdere ondersteunde LXD-releasebranches en MicroCloud-omgevingen.

# Oplossingen

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

# Referenties

- https://discourse.ubuntu.com/t/security-advisory-critical-vulnerability-found-in-canonical-lxd-and-microcloud/90557

# Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2026-112816 | 10.0 CRITICAL |

# CWE's

| CWE | Beschrijving |
| --- | --- |
| CWE-295 | Improper Certificate Validation |

# Getroffen producten

| Canonical |
| --- |
| LXD |

| Debian |
| --- |
| lxd |

# 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.