



NCSC-2025-0265

Kwetsbaarheden verholpen in Commvault

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 20-08-2025

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

Commvault heeft kwetsbaarheden verholpen in Commvault componenten als CommCell en ComServe versies voor 11.36.60.

Duiding

De kwetsbaarheden bevinden zich in versies van Commvault vóór 11.36.60. De eerste kwetsbaarheid stelt niet-geauthenticeerde aanvallers in staat om API-aanroepen uit te voeren via een bekend inlogmechanisme, wat kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens of functionaliteiten binnen de Commvault-omgeving. De tweede kwetsbaarheid betreft een pad-traversal probleem dat door externe aanvallers kan worden misbruikt, wat kan leiden tot ongeautoriseerde toegang tot het bestandssysteem en mogelijk tot remote code execution. De derde kwetsbaarheid is het gevolg van onvoldoende invoervalidatie, waardoor aanvallers commandoregelargumenten kunnen manipuleren, wat hen mogelijk toegang kan geven tot een geldige gebruikerssessie met lage privileges. Deze kwetsbaarheden verhogen het risico op datacompromittatie en schendingen van de systeemintegriteit.

Oplossingen

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

Referenties

- https://documentation.commvault.com/securityadvisories/CV_2025_08_1.html
- https://documentation.commvault.com/securityadvisories/CV_2025_08_2.html
- https://documentation.commvault.com/securityadvisories/CV_2025_08_3.html

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-57788	6.9 MEDIUM
➤ CVE-2025-57790	8.7 HIGH
➤ CVE-2025-57791	6.9 MEDIUM

CWE's

CWE	Beschrijving
> CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
> CWE-259	Use of Hard-coded Password
> CWE-36	Absolute Path Traversal

Getroffen producten

Commvault
CommCell

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.