Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0138

Kwetsbaarheid verholpen in Commvault Command Center

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 06-05-2025
Revisie: 1.0.1

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

Update Revisie 1

Actief misbruik door CISA waargenomen van CVE-2025-34028.

Feiten

Commvault heeft een kwetsbaarheid verholpen in Command Center.

Duiding

De kwetsbaarheid kan door een ongeauthenticeerde kwaadwillende op afstand worden misbruikt voor het uitvoeren van willekeurige code. Hiertoe dient een speciaal vervaardigd http-verzoek naar de kwetsbare applicatie te worden verstuurd met daarin een verwijzing naar een malafide zip-bestand. De kwetsbare applicatie downloadt vervolgens dit zip-bestand en pakt de bestanden die daarin staan uit. Op die manier kan de kwaadwillende via bijvoorbeeld een webshell code op het kwetsbare systeem uitvoeren. CISA heeft op 02-05-2025 aangegeven dat de kwetsbaarheid actief wordt misbruikt.

Oplossingen

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

Referenties

- https://documentation.commvault.com/securityadvisories/CV_2025_04_1.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-34028
- https://www.cisa.gov/news-events/alerts/2025/05/02/cisa-adds-two-known-exploited-vulnerabilities-catalog

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-34028	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Getroffen producten

Commvault
Command Center
Command Center Innovation Release

Disclaimer