Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0220

Kwetsbaarheden verholpen in Rancher door Rancher Labs

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 03-07-2026

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

Rancher Labs heeft kwetsbaarheden verholpen in Rancher versies 2.13.0 tot en met 2.13.7 en 2.14.0 tot en met 2.14.3.

Duiding

De eerste kwetsbaarheid betreft een SAML authenticatie replay probleem in de Assertion Consumer Service (ACS) handler in Rancher versies 2.14.0 tot, maar niet inclusief 2.14.3. De ACS handler dwingt het eenmalig gebruik van SAML assertions niet af, waardoor een aanvaller onderschepte assertions kan hergebruiken. Dit kan leiden tot man-in-the-middle aanvallen die de integriteit van het authenticatieproces aantasten. De tweede kwetsbaarheid zit in de legacy Project Role Template Binding reconciler in Rancher versies 2.13.0 tot en met 2.13.7 en 2.14.0 tot en met 2.14.3. Door het ontbreken van een opruimstap kunnen gebruikers Pod Security Admission permissies behouden die eigenlijk ingetrokken hadden moeten worden wanneer een beheerder deze permissies uit een RoleTemplate verwijdert. Dit komt doordat de reconciler permissies niet correct bijwerkt of verwijdert, waardoor ongeautoriseerde toegang kan blijven bestaan en gebruikers mogelijk verhoogde privileges behouden buiten hun toegestane scope.

Oplossingen

Rancher Labs heeft updates uitgebracht om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/rancher/rancher/security/advisories/GHSA-c4rp-wgqc-mfhc
- https://github.com/rancher/rancher/security/advisories/GHSA-c5jm-xcmq-9j95

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-44946	9.5 CRITICAL
CVE-2026-44947	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-281	Improper Preservation of Permissions
CWE-294	Authentication Bypass by Capture-replay

Getroffen producten

Rancher
Rancher

Disclaimer