



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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.

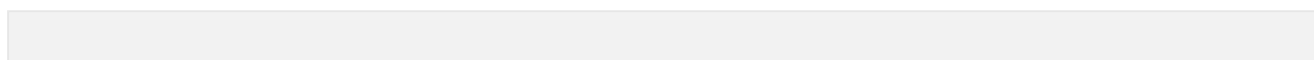
## Referenties

- <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
➤ <a href="#">CVE-2026-44946</a>	9.5 CRITICAL
➤ <a href="#">CVE-2026-44947</a>	6.9 MEDIUM

## CWE's



CWE	Beschrijving
<a href="#">&gt; CWE-281</a>	Improper Preservation of Permissions
<a href="#">&gt; CWE-294</a>	Authentication Bypass by Capture-replay

## Getroffen producten

Rancher
Rancher

## 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.