



# NCSC-2025-0200

## Kwetsbaarheden verholpen in IBM QRadar SIEM

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 20-06-2025

**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](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

IBM heeft kwetsbaarheden verholpen in IBM QRadar SIEM (Specifiek voor versie 7.5.0 Update Package 12).

## Duiding

De kwetsbaarheden omvatten een mogelijkheid voor een bevoegde gebruiker om kritieke configuratiebestanden te wijzigen, wat kan leiden tot het uploaden van schadelijke autoupdatebestanden en het uitvoeren van willekeurige commando's binnen het systeem. Daarnaast is er een kwetsbaarheid gerelateerd aan een XML externe entiteit injectie (XXE) aanval, die kan leiden tot ongeautoriseerde toegang tot gevoelige informatie of uitputting van geheugbronnen. Ook kan gevoelige informatie worden opgeslagen in logbestanden die toegankelijk zijn voor lokale gebruikers, wat het risico op ongeautoriseerde gegevensblootstelling met zich meebrengt.

## Oplossingen

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

## Referenties

➤ <https://www.ibm.com/support/pages/node/7237317>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-33117</a>	8.6 HIGH
➤ <a href="#">CVE-2025-33121</a>	5.3 MEDIUM
➤ <a href="#">CVE-2025-36050</a>	4.8 MEDIUM

## CWE's

CWE	Beschrijving
➤ <a href="#">CWE-611</a>	Improper Restriction of XML External Entity Reference

➤ <a href="#">CWE-73</a>	External Control of File Name or Path
➤ <a href="#">CWE-532</a>	Insertion of Sensitive Information into Log File

## Getroffen producten

### IBM

QRadar  
SIEM

## 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.