



NCSC-2025-0344

Kwetsbaarheden verholpen in Rockwell Automation COMMS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 31-10-2025

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

Rockwell Automation heeft kwetsbaarheden verholpen in COMMS NATR systemen.

Duiding

De kwetsbaarheden omvatten meerdere gebroken authenticatieproblemen die ernstige risico's met zich meebrengen, waaronder denial-of-service aanvallen, mogelijke overnames van admin-accounts en onjuiste wijzigingen in NAT-regels. Daarnaast is er een Stored Cross-Site Scripting kwetsbaarheid die voortkomt uit inadequate filtering en codering van speciale tekens, wat kan leiden tot ongeautoriseerde gegevensmanipulatie en serviceonderbrekingen. Ook is er een Cross-Site Request Forgery (CSRF) probleem dat aanvallers in staat stelt om systeemconfiguraties te wijzigen door een ingelogde administrator te misleiden. Deze kwetsbaarheden kunnen de communicatie van apparaten ernstig verstoren en vereisen mogelijk fysieke toegang om normale operaties te herstellen.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de productieomgeving. Het is goed gebruik een dergelijke omgeving niet publiek toegankelijk te hebben.

Oplossingen

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

Referenties

➤ <https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1756.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-7328	9.9 CRITICAL
➤ CVE-2025-7329	8.5 HIGH
➤ CVE-2025-7330	7.0 HIGH

CWE's

CWE	Beschrijving
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-306	Missing Authentication for Critical Function
> CWE-352	Cross-Site Request Forgery (CSRF)

Getroffen producten

Rockwell Automation
1783-NATR Firmware (OS)
Comms - 1783-NATR

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.