



NCSC-2024-0495

Kwetsbaarheden verholpen in Rockwell Automation Power Monitor 1000

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 19-12-2024

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 de Power Monitor 1000.

Duiding

De kwetsbaarheden bevinden zich in de API van de Power Monitor 1000, waardoor ongeautoriseerde gebruikers nieuwe Policyholder-gebruikers kunnen configureren met hoge privileges. Dit stelt aanvallers in staat om bestaande gebruikers te bewerken, nieuwe beheerders aan te maken en fabrieksinstellingen uit te voeren. Daarnaast kan een andere kwetsbaarheid leiden tot heap-geheugenbeschadiging, wat mogelijk op afstand uitvoeren van willekeurige code of Denial-of-Service-omstandigheden kan veroorzaken.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de productie-infrastructuur. Het is goed gebruik een dergelijke infrastructuur 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.SD1714.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-12371	
➤ CVE-2024-12372	

CWE's

CWE	Beschrijving
➤ CWE-420	Unprotected Alternate Channel
➤ CWE-306	Missing Authentication for Critical Function

> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-122	Heap-based Buffer Overflow

Getroffen producten

rockwellautomation

powermonitor_1000_firmware

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.