Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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