



NCSC-2025-0326

Kwetsbaarheden verholpen in Moxa's netwerkbeveiligingsapparaten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 20-10-2025

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

Moxa heeft kwetsbaarheden verholpen in hun netwerkbeveiligingsapparaten.

Duiding

De kwetsbaarheden in Moxa's netwerkbeveiligingsapparaten omvatten een onjuiste autorisatie die ongeautoriseerde toegang tot beschermde API-eindpunten mogelijk maakt, evenals een probleem met toegangscontrolemechanismen dat kan leiden tot privilege-escalatie. Daarnaast kunnen laaggeprivilegieerde gebruikers administratieve functies uitvoeren, wat interne netwerkverkenning kan vergemakkelijken. Een kritieke kwetsbaarheid stelt laaggeprivilegieerde gebruikers in staat om nieuwe administratoraccounts te creëren, wat volledige administratieve controle en accountimpersonatie mogelijk maakt. Bovendien kunnen ongeauthenticeerde aanvallers hard-coded inloggegevens misbruiken om JSON Web Tokens te vervalsen, wat leidt tot ongeautoriseerde toegang tot de systemen.

Oplossingen

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

Referenties

➤ <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-258121-cve-2025-6892%2C-cve-2025-6893%2C-cve-2025-6894%2C-cve-2025-6949%2C-cve-2025-6950-multiple-vulnerabilities-in-netwo>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-6892	9.4 CRITICAL
➤ CVE-2025-6893	9.3 CRITICAL
➤ CVE-2025-6894	5.3 MEDIUM
➤ CVE-2025-6949	9.3 CRITICAL
➤ CVE-2025-6950	9.9 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-250	Execution with Unnecessary Privileges
➤ CWE-798	Use of Hard-coded Credentials
➤ CWE-863	Incorrect Authorization

Getroffen producten

Moxa
EDF-G1002-BP Series
EDR-8010 Series
EDR-G9010 Series
NAT-102 Series
NAT-108 Series
OnCell G4302-LTE4 Series
Router
TN-4900 Series
edf-g1002- bp
edr-8010
oncell_g4302- lte4
tn-4900

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.