Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2025-0002

Kwetsbaarheden verholpen in Moxa's cellulaire routers en netwerkbeveiligingsapparaten

2025-01-06 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Moxa heeft kwetsbaarheden verholpen in Moxa's cellulaire routers en netwerkbeveiligingsapparaten (Specifiek voor CVE-2024-9138 en CVE-2024-9140).

Interpretaties

De kwetsbaarheid CVE-2024-9138 betreft hard-coded credentials die geauthenticeerde gebruikers in staat stellen hun privileges te escaleren, wat uiteindelijk leidt tot root-toegang. Dit vormt een aanzienlijk risico voor de beveiliging van de getroffen apparaten. Daarnaast stelt CVE-2024-9140 een OS command injection mogelijk, wat leidt tot willekeurige code-executie op de getroffen apparaten.

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-241155-privilege-escalation-and-os-command-injection-vulnerabilities-in-cellular-routers,-secure-routers,-and-netwo