



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans les produits Moxa
<b>Numéro de Référence</b>	63592804/26
<b>Date de Publication</b>	28 Avril 2026
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- TN-4900 Series versions antérieures à v3.24
- OnCell G4308-LTE4 Series versions antérieures ou égales à v3.23.0 sans le dernier correctif de sécurité
- OnCell G4302-LTE4 Series versions antérieures ou égales à v3.23.0 sans le dernier correctif de sécurité
- EDR-G9010 Series versions antérieures à v3.24
- EDR-8010 Series versions antérieures à v3.24
- EDF-G1002-BP Series versions antérieures à v3.24

### Identificateurs externes

- CVE-2020-11868 CVE-2024-7695 CVE-2024-9404 CVE-2025-0415 CVE-2025-0676
- CVE-2025-1679 CVE-2025-1680 CVE-2025-6892 CVE-2025-6893 CVE-2025-6894
- CVE-2025-6949 CVE-2025-6950 CVE-2026-3867 CVE-2026-3868

### Bilan de la vulnérabilité

Moxa a corrigé plusieurs vulnérabilités affectant les équipements réseau susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant de contourner la politique de sécurité, de provoquer un déni de service et de porter atteinte à la confidentialité des données.

### Solution :

Veillez se référer au bulletin de sécurité Moxa du 27 Avril 2026.

### Risque :

- Déni de service,
- Contournement de la politique de sécurité,
- Atteinte à la confidentialité des données,

## Annexe

Bulletin de sécurité Moxa du 27 Avril 2026:

- <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-240933-cve-2024-9404-denial-of-service-vulnerability-identified-in-multiple-pt-switches>
- <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-240162-cve-2024-7695-out-of-bounds-write-vulnerability-identified-in-multiple-pt-switches>
- <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-258121-cve-2025-6892,-cve-2025-6893,-cve-2025-6894,-cve-2025-6949,-cve-2025-6950-multiple-vulnerabilities-in-netwo>
- <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>
- [https://www.moxa.com/en/support/product-support/security-advisory/mpsa-259491-cve-2025-0415-command-injection-leading-to-denial-of-service-\(dos\)](https://www.moxa.com/en/support/product-support/security-advisory/mpsa-259491-cve-2025-0415-command-injection-leading-to-denial-of-service-(dos))
- <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-251431-cve-2025-0676-command-injection-leading-to-privilege-escalation>
- <https://www.moxa.com/en/support/product-support/security-advisory/mpsa-261521-cve-2026-3867-cve-2026-3868-improper-ownership-management-and-improper-handling-of-length-parameter-incons>