DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 12-11-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Cisco
Réference	1270
Date de Publication	2024-11-12
Sévérité	Critique

IMPACT :

- Déni de service à distance
- Exécution de code arbitraire à distance

SYSTÉME AFFECTÉ :

- Enterprise Chat and Email versions 12.6 antérieures à 12.6(1) ES9 ET3
- Enterprise Chat and Email versions antérieures à 12.5(1) ES9
- Nexus Dashboard Fabric Controller versions antérieures à 12.2.2
- Unified Industrial Wireless versions antérieures à 17.15.1

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans les produits Cisco, permettant à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service à distance.

SOLUTION :

Consultez le bulletin de sécurité de l'éditeur pour obtenir les correctifs nécessaires (voir section Documentation).

DOCUMENTATION :

- Bulletin de sécurité Cisco cisco-sa-backhaul-ap-cmdinj-R7E28Ecs du 06 novembre 2024

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs

- Bulletin de sécurité Cisco cisco-sa-ece-dos-Oqb9uFEv du 06 novembre 2024

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-Oqb9uFEv

- Bulletin de sécurité Cisco cisco-sa-ndfc-sqli-CyPPAxrL du 06 novembre 2024

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-sqli-CyPPAxrL

- CVE-2024-20418

https://www.cve.org/CVERecord?id=CVE-2024-20418

- CVE-2024-20484

https://www.cve.org/CVERecord?id=CVE-2024-20484

- CVE-2024-20536

https://www.cve.org/CVERecord?id=CVE-2024-20536