



BULLETIN DE SECURITE

| | |
|----------------------------|---|
| Titre | Vulnérabilité affectant des produits d'ESET |
| Numéro de Référence | 45322212/23 |
| Date de Publication | 22 Décembre 2023 |
| Risque | Important |
| Impact | Important |

Systemes affectés

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate
- ESET Endpoint Antivirus for Windows et ESET Endpoint Security for Windows
- ESET Endpoint Antivirus for Linux 10.0 et versions antérieures
- ESET Server Security for Windows Server (File Security for Microsoft Windows Server), ESET Mail Security for Microsoft Exchange Server, ESET Mail Security for IBM Domino, ESET Security for Microsoft SharePoint Server, ESET File Security for Microsoft Azure
- ESET Server Security for Linux 10.1 et versions antérieures

Identificateurs externes

- CVE-2023-5594

Bilan de la vulnérabilité

ESET annonce la disponibilité de mises à jour qui permettant la correction d'une vulnérabilité affectant certains de ses produits. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'accéder à des données confidentielles.

Solution

Veillez se référer au bulletin de sécurité d'ESET pour obtenir les mises à jour.

Risque

- Accès à des données confidentielles

Référence

Bulletin de sécurité d'ESET :

- <https://support.eset.com/en/ca8562-eset-customer-advisory-improper-following-of-a-certificates-chain-of-trust-in-eset-security-products-fixed>