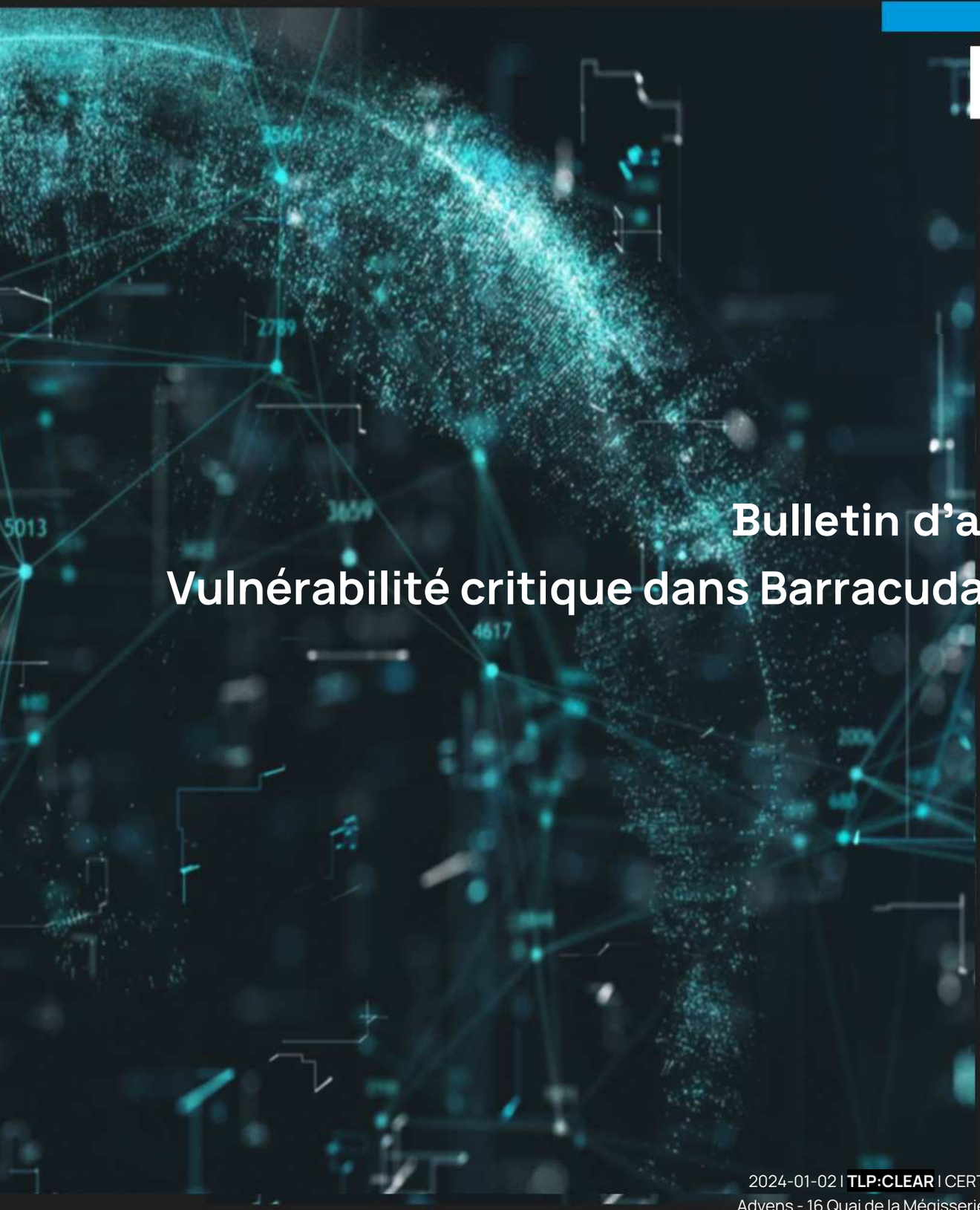
aDvens

Security for the greater good



Bulletin d’alerte

Vulnérabilité critique dans Barracuda ESG

2024-01-02 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

BARRACUDA NETWORKS

Le 24 décembre 2023, Barracuda a publié un bulletin concernant une vulnérabilité **exploitée** dans ESG, son outil de filtrage de sécurité des e-mails.

Barracuda ESG - CVE-2023-7102

Des chercheurs en sécurité ont découvert un défaut d'injection de commande dans la bibliothèque tierce *Spreadsheet::ParseExcel*. Cette dernière est une bibliothèque *open source* utilisée par l'antivirus Amavis au sein de l'application Barracuda ESG.

L'exploitation de cette faille par un attaquant distant et non authentifié permet, en déployant une pièce jointe Excel spécifiquement forgée, d'exécuter du code arbitraire.

L'éditeur mentionne que la vulnérabilité est activement exploitée.

Type de vulnérabilité

- **CWE-1104**: Use of Unmaintained Third Party Components

Risques

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produit impacté

- Barracuda ESG versions comprises à 5.1.3.001 et 9.2.1.001 (incluse).

Recommandations

Barracuda a déployé une mise à jour automatique des instances ESG actives le 21 décembre 2023. Aucune action de la part des utilisateurs n'est nécessaire.

Sur la base de la constatation de l'exploitation de la CVE par l'APT UNC4841 et de l'utilisation de nouvelles variantes des maliciels SEASPY et SALTWATER, l'éditeur a déployé le 22 décembre 2023 un correctif sur les instances ESG compromises présentant des IOCs en lien avec ces nouveaux variants. Aucune action n'est requise de la part des utilisateurs.

Barracuda Networks a déposé deux CVEs différentes :

- La CVE-2023-7101 est dédiée à la vulnérabilité affectant le module Spreadsheet::ParseExcel seul,
- La CVE-2023-7102 est dédiée à la faille affectant Barracuda ESG via *Spreadsheet::ParseExcel* et son exploitation.

Il est recommandé de mettre à jour le module Spreadsheet::ParseExcel vers sa version 0.66.

Site de l'éditeur

- Des informations complémentaires sont disponibles sur le bulletin Barracuda.

Preuve de concept

Une preuve de concept est disponible en source ouverte.

Références

BARRACUDA

- https://www.barracuda.com/company/legal/esg-vulnerability

CVE-2023-7102

- https://nvd.nist.gov/vuln/detail/CVE-2023-7102
- https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2023/MNDT-2023-0019.md
- https://metacpan.org/dist/Spreadsheet-ParseExcel