aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans Symantec

2024-01-26 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Symantec

Le 25 janvier 2024, Exodus Intelligence a publié quatre bulletins de sécurité concernant les vulnérabilités critiques CVE-2024-23613, CVE-2024-23614, CVE-2024-23615 et CVE-2024-23616 sur Symantec.

CVE-2024-23613

Cette vulnérabilité est due à un défaut de contrôle de la mémoire lors du traitement de jetons *UpdateComputer* de Symantec Deployment Solution.

En envoyant des requêtes spécifiquement forgées, un attaquant non authentifié peut exécuter du code arbitraire avec les privilèges *SYSTEM*.

Type de vulnérabilité

- CWE-119 : Improper Restriction of Operations within the Bounds of a Memory Buffer

Risques

- Exécution de code arbitraire
- Elévation de privilèges

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
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

Produits impactés

- Selon Exodus Intelligence, Symantec Deployment Solution version 7.9 est impacté.

Recommandations

- Ce produit étant en fin de vie, aucun correctif n'est disponible.
- Il est recommandé d'utiliser un produit maintenu par l'éditeur.
- Des informations complémentaires sont disponibles dans le bulletin d'Exodus Intelligence.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

CVE-2024-23614

Cette vulnérabilité est due à un défaut de contrôle de la mémoire dans Symantec Messaging Gateway.

En envoyant des requêtes spécifiquement forgées, un attaquant non authentifié peut exécuter du code arbitraire avec les privilèges *root*.

Type de vulnérabilité

- CWE-119 : Improper Restriction of Operations within the Bounds of a Memory Buffer

Risques

- Exécution de code arbitraire
- Elévation de privilèges

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
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

Produits impactés

- Selon Exodus Intelligence, Symantec Messaging Gateway versions 9.5 et antérieures sont impactées.

Recommandations

- Ce produit étant en fin de vie, aucun correctif n'est disponible.
- Il est recommandé d'utiliser un produit maintenu par l'éditeur.
- Des informations complémentaires sont disponibles dans le bulletin d'Exodus Intelligence.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

CVE-2024-23615

Cette vulnérabilité est due à un défaut de contrôle de la mémoire dans Symantec Messaging Gateway.

En envoyant des requêtes spécifiquement forgées, un attaquant non authentifié peut exécuter du code arbitraire avec les privilèges *root*.

Type de vulnérabilité

- CWE-119 : Improper Restriction of Operations within the Bounds of a Memory Buffer

Risques

- Exécution de code arbitraire
- Elévation de privilèges

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
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

Produits impactés

- Selon Exodus Intelligence, Symantec Messaging Gateway versions 9.5 et antérieures sont impactées.

Recommandations

- Ce produit étant en fin de vie, aucun correctif n'est disponible.
- Il est recommandé d'utiliser un produit maintenu par l'éditeur.
- Des informations complémentaires sont disponibles dans le bulletin d'Exodus Intelligence.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

CVE-2024-23616

Cette vulnérabilité est due à un défaut de contrôle de la mémoire dans Symantec Server Management Suite.

En envoyant des requêtes spécifiquement forgées, un attaquant non authentifié peut exécuter du code arbitraire avec les privilèges *SYSTEM*.

Type de vulnérabilité

- CWE-119 : Improper Restriction of Operations within the Bounds of a Memory Buffer

Risques

- Exécution de code arbitraire
- Elévation de privilèges

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
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

Produits impactés

- Selon Exodus Intelligence, Symantec Server Management Suite version 7.9 et antérieures sont impactées.

Recommandations

- Ce produit étant en fin de vie, aucun correctif n'est disponible.
- Il est recommandé d'utiliser un produit maintenu par l'éditeur.
- Des informations complémentaires sont disponibles dans le bulletin d'Exodus Intelligence.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

Références

CVE-2024-23613

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23613
- https://blog.exodusintel.com/2024/01/25/symantec-deployment-solution-axengine-exe-buffer-overflow-remote-code-execution/

CVE-2024-23614

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23614
- https://blog.exodusintel.com/2024/01/25/symantec-messaging-gateway-stack-buffer-overflow-remote-code-execution/

CVE-2024-23615

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23615
- https://blog.exodusintel.com/2024/01/25/symantec-messaging-gateway-libdec2lha-so-stack-buffer-overflow-remote-code-execution/

CVE-2024-23616

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23616
- https://blog.exodusintel.com/2024/01/25/symantec-server-management-suite-axengine-exe-buffer-overflow-remote-code-execution/