

A background visualization of a network or data flow, featuring a dense web of blue and white nodes connected by thin lines, with some nodes highlighted in a brighter blue. The overall aesthetic is futuristic and technical.

Bulletin d'alerte Vulnérabilité critique dans Symantec

Sommaire

SYMANTEC	2
CVE-2024-23613	2
Type de vulnérabilité.....	2
Risques.....	2
Criticité (score de base CVSS v3.1).....	2
Produits impactés.....	2
Recommandations.....	2
Preuve de concept.....	2
CVE-2024-23614	3
Type de vulnérabilité.....	3
Risques.....	3
Criticité (score de base CVSS v3.1).....	3
Produits impactés.....	3
Recommandations.....	3
Preuve de concept.....	3
CVE-2024-23615	4
Type de vulnérabilité.....	4
Risques.....	4
Criticité (score de base CVSS v3.1).....	4
Produits impactés.....	4
Recommandations.....	4
Preuve de concept.....	4
CVE-2024-23616	5
Type de vulnérabilité.....	5
Risques.....	5
Criticité (score de base CVSS v3.1).....	5
Produits impactés.....	5
Recommandations.....	5
Preuve de concept.....	5
RÉFÉRENCES	6

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
- élévation 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/>