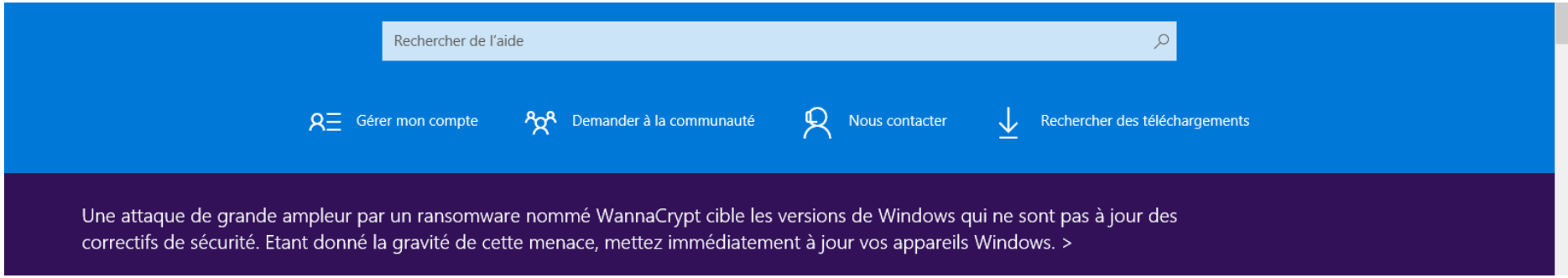

Bulletin de sécurité Microsoft MS17-010 - Critique

https://technet.microsoft.com/library/security/ms17-010.aspx

Mise à jour de sécurité pour le serveur SMB Microsoft Windows (4013389)

Date de publication : 14 mars 2017

Version : 1.0

Sur cette page

- Révisions

Synthèse

Cette mise à jour de sécurité corrige des vulnérabilités dans Microsoft Windows. La plus grave de ces vulnérabilités pourrait permettre l'exécution de code à distance si un attaquant envoyait des messages spécialement conçus à un serveur Windows SMBv1.

Cette mise à jour de sécurité est de niveau « Critique » pour toutes les versions prises en charge de Microsoft Windows. Pour plus d'informations, consultez la section **Logiciels concernés et indices de gravité de la vulnérabilité**.

La mise à jour de sécurité corrige les vulnérabilités en modifiant la manière dont SMBv1 traite les requêtes spécialement conçues.

Pour plus d'informations sur les vulnérabilités, consultez la section **Informations par vulnérabilité**.

Pour plus d'informations sur cette mise à jour, consultez l'article 4013389 de la Base de connaissances Microsoft.

Logiciels concernés et indices de gravité de la vulnérabilité

Les versions ou éditions répertoriées ci-dessous sont concernées. Les versions ou éditions non répertoriées ont atteint la fin de leur cycle de vie ou ne sont pas concernées. Consultez le site web Politique de Support Microsoft afin de connaître la politique de support Microsoft pour votre version ou édition.

Les indices de gravité indiqués pour chaque logiciel concerné supposent l'impact potentiel maximal de la vulnérabilité. Pour plus d'informations sur les risques dans les 30 jours suivant la publication d'un Bulletin concernant l'exploitabilité de la vulnérabilité par rapport à son indice de gravité et à son impact, consultez l'Indice d'exploitabilité dans la synthèse des Bulletins de sécurité de mars.

Remarque Consultez le guide des mises à jour de sécurité pour découvrir la nouvelle approche concernant l'utilisation des informations sur les mises à jour de sécurité. Vous pouvez personnaliser les vues et créer des feuilles de calcul sur les logiciels concernés, ainsi que télécharger des données via une API RESTful. Pour plus d'informations, consultez le Forum aux questions concernant le guide des mises à jour de sécurité. Pour rappel, le guide des mises à jour de sécurité remplacera les Bulletins de sécurité. Pour plus d'informations, consultez notre billet de blog Furthering our commitment to security updates (en anglais uniquement).

Système d'exploitation	Vulnérabilité d'exécution de code à distance sur serveur SMB Windows - CVE-2017-0143	Vulnérabilité d'exécution de code à distance sur serveur SMB Windows - CVE-2017-0144	Vulnérabilité d'exécution de code à distance sur serveur SMB Windows - CVE-2017-0145	Vulnérabilité d'exécution de code à distance sur serveur SMB Windows - CVE-2017-0146	Vulnérabilité de divulgation d'informations sur serveur SMB Windows - CVE-2017-0147	Vulnérabilité d'exécution de code à distance sur serveur SMB Windows - CVE-2017-0148	Mises à jour remplacées
Windows Vista							
Windows Vista Service Pack 2 (4012598)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3177186 dans le Bulletin MS16-114
Windows Vista Édition x64 Service Pack 2 (4012598)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3177186 dans le Bulletin MS16-114
Windows Server 2008							
Windows Server 2008 pour systèmes 32 bits Service Pack 2 (4012598)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3177186 dans le Bulletin MS16-114
Windows Server 2008 pour systèmes x64 Service Pack 2 (4012598)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3177186 dans le Bulletin MS16-114

Windows Server 2008 pour systèmes Itanium Service Pack 2 (4012598)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3177186 dans le Bulletin MS16-114
Windows 7							
Windows 7 pour systèmes 32 bits Service Pack 1 (4012212) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows 7 pour systèmes 32 bits Service Pack 1 (4012215) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3212646
Windows 7 pour systèmes x64 Service Pack 1 (4012212) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows 7 pour systèmes x64 Service Pack 1 (4012215) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3212646
Windows Server 2008 R2							

Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (4012212) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (4012215) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3212646
Windows Server 2008 R2 pour systèmes Itanium Service Pack 1 (4012212) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows Server 2008 R2 pour systèmes Itanium Service Pack 1 (4012215) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3212646
Windows 8.1							

Windows 8.1 pour systèmes 32 bits (4012213) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows 8.1 pour systèmes 32 bits (4012216) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3205401
Windows 8.1 pour systèmes x64 (4012213) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows 8.1 pour systèmes x64 (4012216) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3205401
Windows Server 2012 et Windows Server 2012 R2							
Windows Server 2012 (4012214) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows Server 2012 (4012217) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3205409

Windows Server 2012 R2 (4012213) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows Server 2012 R2 (4012216) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3205401
Windows RT 8.1							
Windows RT 8.1[2] (4012216) Correctif cumulatif mensuel	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3205401
Windows 10							
Windows 10 pour systèmes 32 bits [3] (4012606)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3210720
Windows 10 pour systèmes x64 [3] (4012606)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3210720
Windows 10 version 1511 pour systèmes 32 bits [3] (4013198)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3210721
Windows 10 version 1511 pour systèmes x64 [3] (4013198)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3210721

Windows 10 version 1607 pour systèmes 32 bits [3] (4013429)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3213986
Windows 10 version 1607 pour systèmes x64 [3] (4013429)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3213986
Windows Server 2016							
Windows Server 2016 pour systèmes x64 [3] (4013429)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3213986
Option d'installation Server Core							
Windows Server 2008 pour systèmes 32 bits Service Pack 2 (installation Server Core) (4012598)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3177186 dans le Bulletin MS16-114
Windows Server 2008 pour systèmes x64 Service Pack 2 (installation Server Core) (4012598)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3177186 dans le Bulletin MS16-114
Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (installation Server Core) (4012212)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune

Sécurité uniquement[1]							
Windows Server 2008 R2 pour systèmes x64 Service Pack 1 (installation Server Core) (4012215) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3212646
Windows Server 2012 (installation Server Core) (4012214) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune
Windows Server 2012 (installation Server Core) (4012217) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3205409
Windows Server 2012 R2 (installation Server Core) (4012213) Sécurité uniquement[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	Aucune

Windows Server 2012 R2 (installation Server Core) (4012216) Correctif cumulatif mensuel[1]	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3205401
Windows Server 2016 pour systèmes x64 [3] (installation Server Core) (4013429)	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Critique** Exécution de code à distance	**Important** Divulgation d'informations	**Critique** Exécution de code à distance	3213986

[1] Depuis octobre 2016, Microsoft a modifié le modèle de maintenance des mises à jour pour Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 et Windows Server 2012 R2. Pour plus d'informations, consultez cet article de Microsoft TechNet.

[2] Cette mise à jour n'est disponible que via Windows Update.

[3] Les mises à jour de Windows 10 et Windows Server 2016 sont cumulatives. La mise à jour de sécurité mensuelle comprend tous les correctifs de sécurité pour des vulnérabilités qui concernent Windows 10, en plus de mises à jour non liées à la sécurité. Les mises à jour sont disponibles via le Catalogue Microsoft Update. À partir du 13 décembre 2016, les informations concernant Windows 10 et Windows Server 2016 pour les mises à jour cumulatives seront documentées dans les notes de publication. Consultez les notes de publication en ce qui concerne les numéros de build du système d'exploitation, les problèmes connus et la liste de fichiers concernés.

*La colonne Mises à jour remplacées n'affiche que la dernière mise à jour d'une série de mises à jour remplacées. Pour obtenir la liste complète des mises à jour remplacées, accédez au Catalogue Microsoft Update, recherchez le numéro d'article de la Base de connaissances, puis consultez les détails de la mise à jour (les informations sur les mises à jour remplacées figurent sous l'onglet Détails du package).

Informations par vulnérabilité

Vulnérabilités d'exécution de code à distance sur serveur SMB Windows

Il existe des vulnérabilités d'exécution de code à distance quant à la manière dont le serveur Microsoft Server Message Block 1.0 (SMBv1) traite certaines requêtes. Un attaquant qui parviendrait à exploiter ces vulnérabilités pourrait exécuter du code sur le serveur cible.

Dans la plupart des cas, pour exploiter ces vulnérabilités, un attaquant non authentifié pourrait envoyer un paquet spécialement conçu à un serveur SMBv1 ciblé.

La mise à jour de sécurité corrige les vulnérabilités en modifiant la manière dont SMBv1 traite ces requêtes spécialement conçues.

Le tableau suivant contient des liens vers l'entrée standard correspondant à chaque vulnérabilité dans la liste de CVE (Common Vulnerabilities and Exposures) :

Titre de la vulnérabilité	Numéro CVE	Révélée publiquement	Exploitée
Vulnérabilité d'exécution de code à distance sur serveur SMB Windows	CVE-2017-0143	Non	Non
Vulnérabilité d'exécution de code à distance sur serveur SMB Windows	CVE-2017-0144	Non	Non
Vulnérabilité d'exécution de code à distance sur serveur SMB Windows	CVE-2017-0145	Non	Non
Vulnérabilité d'exécution de code à distance sur serveur SMB Windows	CVE-2017-0146	Non	Non
Vulnérabilité d'exécution de code à distance sur serveur SMB Windows	CVE-2017-0148	Non	Non

Facteurs atténuants

Microsoft n'a identifié aucun facteur atténuant pour ces vulnérabilités.

Solutions de contournement

Les solutions de contournement suivantes peuvent être utiles, selon votre situation :

- **Désactiver SMBv1**

Pour les clients exécutant Windows Vista et versions ultérieures

Voir l'article 2696547 de la Base de connaissances Microsoft.

Méthode alternative pour les clients utilisant Windows 8.1 ou Windows Server 2012 R2 et versions ultérieures

Pour les systèmes d'exploitation client :

1. Ouvrez le **Panneau de configuration**, cliquez sur **Programmes**, puis cliquez sur **Activer ou désactiver des fonctionnalités Windows**.
2. Dans la fenêtre Fonctionnalités de Windows, désactivez la case **Support de partage de fichiers SMB 1.0/CIFS**, puis cliquez sur **OK** pour fermer la fenêtre.
3. Redémarrez le système.

Pour les systèmes d'exploitation serveur :

4. Ouvrez le **Gestionnaire de serveur**, cliquez sur le menu **Gérer**, puis sélectionnez **Ajouter ou supprimer des rôles et des fonctionnalités**.
5. Dans la fenêtre Fonctionnalités, désactivez la case **Support de partage de fichiers SMB 1.0/CIFS**, puis cliquez sur **OK** pour fermer la fenêtre.
6. Redémarrez le système.

Impact de cette solution de contournement. Le protocole SMBv1 est désactivé sur le système cible.

Procédure d'annulation de cette solution de contournement. Effectuez à nouveau les étapes de la solution de contournement, mais activez la fonction Support de partage de fichiers SMB 1.0/CIFS.

Vulnérabilité de divulgation d'informations sur serveur SMB Windows - CVE-2017-0147

Il existe une vulnérabilité de divulgation d'informations quant à la manière dont le serveur Microsoft Server Message Block 1.0 (SMBv1) traite certaines requêtes. Un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait concevoir un paquet spécial pouvant entraîner une divulgation d'informations depuis le serveur.

Dans la plupart des cas, pour exploiter cette vulnérabilité, un attaquant non authentifié pourrait envoyer un paquet spécialement conçu à un serveur SMBv1 ciblé.

La mise à jour de sécurité corrige la vulnérabilité en modifiant la manière dont SMBv1 traite ces requêtes spécialement conçues.

Le tableau suivant contient des liens vers l'entrée standard correspondant à chaque vulnérabilité dans la liste de CVE (Common Vulnerabilities and Exposures) :

Titre de la vulnérabilité	Numéro CVE	Révélée publiquement	Exploitée
Vulnérabilité de divulgation d'informations sur serveur SMB Windows	CVE-2017-0147	Non	Non

Facteurs atténuants

Microsoft n'a identifié aucun facteur atténuant pour cette vulnérabilité.

Solutions

Les solutions de contournement suivantes peuvent être utiles, selon votre situation :

- **Désactiver SMBv1**

  Pour les clients exécutant Windows Vista et versions ultérieures

  Voir l'article 2696547 de la Base de connaissances Microsoft.

  Méthode alternative pour les clients utilisant Windows 8.1 ou Windows Server 2012 R2 et versions ultérieures

Pour les systèmes d'exploitation client :

1. Ouvrez le **Panneau de configuration**, cliquez sur **Programmes**, puis cliquez sur **Activer ou désactiver des fonctionnalités Windows**.
2. Dans la fenêtre Fonctionnalités de Windows, désactivez la case **Support de partage de fichiers SMB 1.0/CIFS**, puis cliquez sur **OK** pour fermer la fenêtre.
3. Redémarrez le système.

Pour les systèmes d'exploitation serveur :

4. Ouvrez le **Gestionnaire de serveur**, cliquez sur le menu **Gérer**, puis sélectionnez **Ajouter ou supprimer des rôles et des fonctionnalités**.
5. Dans la fenêtre Fonctionnalités, désactivez la case **Support de partage de fichiers SMB 1.0/CIFS**, puis cliquez sur **OK** pour fermer la fenêtre.
6. Redémarrez le système.

Impact de cette solution de contournement. Le protocole SMBv1 est désactivé sur le système cible.

Procédure d'annulation de cette solution de contournement. Effectuez à nouveau les étapes de la solution de contournement, mais activez la fonction Support de partage de fichiers SMB 1.0/CIFS.

Déploiement des mises à jour de sécurité

Pour plus d'informations sur le déploiement des mises à jour de sécurité, consultez l'article de la Base de connaissances Microsoft référencé ici dans la synthèse.

Remerciements

Microsoft reconnaît les efforts des professionnels de la sécurité qui contribuent à protéger les clients par une divulgation coordonnée des vulnérabilités. Reportez-vous à la page Remerciements pour plus d'informations.

Dédit de responsabilité

Les informations contenues dans la Base de connaissances Microsoft sont fournies « en l'état », sans garantie d'aucune sorte. Microsoft exclut toute garantie expresse ou implicite, notamment toute garantie de qualité et d'adéquation à un usage particulier. En aucun cas, la société Microsoft ou ses fournisseurs ne pourront être tenus pour responsables de quelque dommage que ce soit, y compris toute perte de bénéfices directe, indirecte ou accessoire, ou de dommages spéciaux, même si la société Microsoft a été prévenue de l'éventualité de tels dommages. Certains pays n'autorisent pas l'exclusion ou la limitation des responsabilités pour les dommages indirects ou accessoires, de sorte que la limitation ci-dessus peut ne pas être applicable.

Révisions

- V1.0 (14 mars 2017) : Bulletin publié.