Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 15 mai 2017
N° CERTFR-2017-ALE-008

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Multiples vulnérabilités dans Microsoft Windows XP et Windows Server 2003

Gestion du document

Référence	CERTFR-2017-ALE-008
Titre	Multiples vulnérabilités dans Microsoft Windows XP et Windows Server 2003
Date de la première version	14 avril 2017
Date de la dernière version	14 juin 2017
Source(s) heightPièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- exécution de code arbitraire à distance
- élévation de privilèges

2 - Systèmes affectés

Microsoft Windows XP et Windows Server 2003, tous services packs confondus

3 - Résumé

De multiples vulnérabilités ont été découvertes dans *Windows XP et Windows Server 2003*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une élévation de privilèges.

4 - Contournement provisoire

Le 14 avril 2017, le groupe d'attaquants Shadowbrokers a publié une nouvelle archive contenant des outils offensifs.
Parmi ceux-ci se trouvent des codes permettant d'exploiter :

Remote Desktop Protocol (RDP)

Un code permet l'exploitation d'une vulnérabilité accessible par le service *Remote Desktop Protocol*.

Le composant affecté correspond au service d'authentification par carte à puce, exposé via l'extension RDP *Smart Card Virtual Channel*. Quand les machines sont membres d'un domaine Active Directory, ce composant est activé par défaut et accessible via le protocole RDP (port TCP 3389).

La vulnérabilité est présente même si l'authentification par carte à puce n'est pas utilisée. Le code d'attaque disponible publiquement permet d'obtenir une exécution de code arbitraire à distance avec les privilèges `SYSTEM`. Le CERT-FR recommande de filtrer l'accès au service RDP (port TCP 3389), que les machines soient accessibles ou non sur internet, afin que seules des machines de confiance puissent s'y connecter. De manière plus générale, le CERT-FR déconseille l'utilisation de systèmes en fin de vie (cf. section Documentation).

Il existe toutefois une mesure de contournement efficace et simple à implémenter. La clé de registre suivante est présente par défaut dans toutes les versions de Windows XP et Windows Server 2003 :

– \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Gemplus GemSAFE Card CSP v1.0.

Supprimer celle-ci rend l'exploitation de cette vulnérabilité impossible. Elle implique cependant un effet de bord car la suppression de cette clé de registre empêche l'utilisation de lecteurs de cartes utilisant les pilotes Gemalto.

Le 13 juin 2017, Microsoft a publié un correctif pour cette vulnérabilité exploitée par le code d'attaque *ESTEEMAUDIT* (cf. section Documentation).

Microsoft Server Message Block (SMB)

Plusieurs codes d'exploitation ciblent le serveur SMB de Windows et permettent une exécution de code arbitraire à distance avec des privilèges élevés (`noyau`).

Le 12 mai 2017, l'une des vulnérabilités SMB a été exploitée dans le cadre d'une campagne de propagation de rançongiciels (cf. section Documentation). Au vu de l'ampleur de la menace et à titre exceptionnel, Microsoft a publié un correctif de sécurité (cf. section Documentation) pour des systèmes qui ne sont plus maintenus depuis de nombreux mois, voire plusieurs années.

L'exploitation avérée à grande échelle de cette vulnérabilité rend d'autant plus critique l'installation des correctifs dans les plus brefs délais et la migration des systèmes obsolètes.

Microsoft Exchange

L'un des codes permet d'obtenir une exécution de code à distance sur les versions de Microsoft Exchange 2007 et antérieures.

Le 13 juin 2017, Microsoft a publié un correctif pour cette vulnérabilité exploitée par le code d'attaque *ENGLISHMANDENTIST* (cf. section Documentation).

Internet Information Services (IIS)

Le module WebDAV du serveur IIS est ciblé par l'un des codes d'exploitation qui permet d'obtenir une exécution de code arbitraire à distance avec les privilèges `SYSTEM`.

Le 13 juin 2017, Microsoft a publié un correctif pour cette vulnérabilité exploitée par le code d'attaque *EXPLODINGCAN* (cf. section Documentation).

Recommandations

Bien que des systèmes comme Microsoft Windows XP et Windows Server 2003 ne sont plus maintenus depuis plusieurs années, force est de constater que leur présence dans les parcs informatiques est toujours non négligeable. Avec la mise à disposition publique de plus en plus de codes d'exploitation ciblant ces systèmes obsolètes, les risques augmentent en conséquence, en particulier pour les systèmes accessibles sur internet.

Même s'il est possible de tenter de réduire la surface d'attaque en filtrant les communications vers les services vulnérables ou en les désactivant, il faut considérer que, d'une manière générale, les systèmes en fin de vie donnent aux attaquants un moyen d'accès ou de déplacement latéral à moindre coût.

Les mesures de sécurité compensatoires devront donc être évaluées et les risques résiduels formellement acceptés. Le CERT-FR insiste sur l'importance de migrer vers des versions maintenues et à jour par les éditeurs (cf. section Documentation).

5 - Documentation

- Avis CERT-FR CERTFR-2017-AVI-181
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-181/index.html
- Avis CERT-FR CERTFR-2017-AVI-154
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-154/index.html
- Alerte CERT-FR CERTFR-2017-ALE-010
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ALE-010/index.html
- Les systèmes et logiciels obsolètes
  http://www.cert.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html

Gestion détaillée du document

14 avril 2017 version initiale.

19 avril 2017 extension de l'alerte à d'autres composants vulnérables.

15 mai 2017 mise à jour de l'alerte pour tenir compte de la campagne de propagation de rançongiciels via une vulnérabilité SMB.

31 mai 2017 ajout d'une mesure de contournement pour le code d'attaque *ESTEEMAUDIT* affectant le protocole RDP.

14 juin 2017 mise à jour de l'alerte pour tenir compte des correctifs publiés par Microsoft concernant les codes d'attaque *ESTEEMAUDIT*, *EXPLODINGCAN* et *ENGLISHMANDENTIST*

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-008`