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 10 avril 2017
N° CERTFR-2017-ACT-015

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-015

1 - Vulnérabilité Microsoft Windows IIS 6.0

Contexte

Le 27 mars 2017, des chercheurs en sécurité ont publié sur Internet un code d'exploitation d'une vulnérabilité portant sur le module WebDav du service IIS 6.0, sur Microsoft Windows Server 2003 R2.

Le module WebDav permet à un utilisateur d'interagir avec des fichiers hébergés sur un serveur IIS. Il s'agit d'une extension du protocole HTTP.

L'organisme MITRE a assigné l'identifiant CVE-2017-7269 à cette vulnérabilité, pour laquelle aucun correctif ne sera publié, Windows Server 2003 R2 n'étant plus soutenu par Microsoft depuis 2015.

Suite à la publication du code d'exploitation, l'éditeur a identifié sur Internet des recherches et des exploitations de cette vulnérabilité à des fins malveillantes.

Nature et impact de la vulnérabilité

L'exploitation de cette vulnérabilité du module WebDav peut permettre une exécution de code arbitraire à distance en forgeant des requêtes spécifiques.

Même si le service IIS 6.0 est par défaut configuré pour s'exécuter dans un compte restreint, il existe plusieurs vulnérabilités publiquement documentées permettant de réaliser une élévation des privilèges et de prendre le contrôle du système visé.

Le module WebDav n'est toutefois pas activé par défaut lors d'une installation de IIS 6.0.

Recommandations

L'ANSSI recommande de désactiver le module WebDav des serveurs IIS 6.0 au plus vite, qu'ils soient exposés sur Internet ou non. La migration des serveurs Windows 2003 vers des versions supportées par l'éditeur doit également être mise en oeuvre.

2 - Rappel des avis émis

Dans la période du 03 au 09 avril 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-098 : Vulnérabilité dans Apple iOS
- CERTFR-2017-AVI-099 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2017-AVI-100 : Multiples vulnérabilités dans SCADA Schneider Electric Modicon

– CERTFR-2017-AVI-101 : Vulnérabilité dans Xen
– CERTFR-2017-AVI-102 : Vulnérabilité dans Asterisk
– CERTFR-2017-AVI-103 : Multiples vulnérabilités dans les produits Cisco
– CERTFR-2017-AVI-104 : Vulnérabilité dans SCADA Schneider Electric IGSS

Durant la même période, les publications suivantes ont été mises à jour :

– CERTFR-2017-AVI-097 : Multiples vulnérabilités dans le noyau Linux de SUSE (ajout des avis de sécurité SUSE SUSE-SU-2017:0912-1 et SUSE-SU-2017:0913-1.)

Gestion détaillée du document

10 avril 2017 version initiale.