Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 03 mai 2013
N° CERTA-2013-ACT-018

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-018

1 Attaques par relais SMB

Les attaques SMB (Server Message Block) sont connues depuis de nombreuses années. En perte de vitesse, elles tendent récemment à revenir sur le devant de la scène.

L'attaque consiste à relayer les demandes de connexions d'un administrateur vers une machine. Lors de l'authentification un jeton est généré par le serveur et permet à un utilisateur de se connecter. Le pirate alors positionné en « homme du milieu » bloque ce jeton et l'utilise pour se connecter à la place de l'administrateur réel. Il est ainsi possible d'usurper une session sans pour autant posséder le mot de passe utilisateur.

Cette attaque a été très utilisée sur le protocole NTLMv1 car elle était implémentée dans plusieurs outils d'audits. Certains administrateurs ont donc forcés l'utilisation de NLMv2 [1], ce qui est une bonne chose en soit, seulement NTLMv2 en l'état reste vulnérable à ce type d'attaques. Le CERTA recommande en plus du NTLMv2 de signer les communication aussi bien du côté client [2] que serveur [3].

Documentation

- Forcer l'utilisation de NTLMv2 :
  `http://technet.microsoft.com/en-us/library/cc738867(v=ws.10).aspx`
- Activer la signature des communications côté client :
  `http://technet.microsoft.com/en-us/library/cc728025(v=ws.10).aspx`
- Activer la signature des communications côté serveur :
  `http://technet.microsoft.com/en-us/library/cc786681(v=ws.10).aspx`

2 Vulnérabilités des greffons des gestionnaires de contenu

Régulièrement des vulnérabilités sont corrigées dans les différents systèmes de gestion de contenu, mais les administrateurs oublient parfois que les greffons de ce gestionnaire peuvent également faire l'objet de failles logicielles.

A titre d'exemple, les greffons *W3 Total Cache* et *WP Super Cache* pour le SGC WordPress ont récemment souffert de vulnérabilités permettant l'exécution de code à distance. La prise de contrôle d'un site peut permettre, par exemple, à un attaquant d'y déposer un kit d'hameçonnage, un kit d'exploitation, un outil de déni de service ou encore de dérober des informations stockées sur celui-ci (*ie.* extraction de base de donnée).

Le CERTA encourage donc à appliquer les mesures suivantes :

- utiliser un système de gestion de contenu maintenu par ses développeurs ;

– tenir à jour le gestionnaire de contenu des correctifs de sécurité ;
– mettre à jour les greffons utilisés dans le gestionnaire ;
– désactiver les greffons inutiles.

3 Switchs et routeurs domestiques, une porte grande ouverte sur votre réseau ?

Dans une étude récente, la société américaine ISE a démontré l'existence de nombreuses vulnérabilités dans différents équipements réseau « domestiques ». Ces équipements (switchs, routeurs, point d'accès, etc.) sont essentiellement destinés aux particuliers ou aux PME n'ayant pas de gros besoins d'infrastructure en système d'information.

Cependant, il n'est pas rare de rencontrer de tels appareils dans des réseaux plus conséquents. En effet, leur simplicité de configurations et leur faible prix en font des candidats idéaux lorsqu'il s'agit d'interconnecter différents réseaux (entres eux ou avec l'Internet), ou bien encore de fournir un point d'accès sans fil à des agents de passage. Ils deviennent ainsi partie intégrante du réseau de l'entreprise et, du fait de leurs vulnérabilités, en augmentent considérablement la surface d'attaque.

Certaines failles découvertes par ISE permettent, en effet, de prendre le contrôle de l'équipement depuis l'Internet, ouvrant ainsi les portes du SI de l'entreprise à un attaquant. De plus, tous les équipements analysés par cette étude souffrent de vulnérabilités permettant à un attaquant, déjà présent sur le LAN, d'en prendre le contrôle, offrant ainsi une position idéale pour l'observation et la modification du trafic réseau (fausses réponses DNS, redirections illégitimes, etc.).

Pour les réseaux d'entreprise, le CERTA recommande de proscrire l'utilisation des équipements réseaux « domestiques » et de privilégier des équipements professionnels qui font l'objet d'un suivi de sécurité, même si ces derniers sont plus onéreux et plus complexes à configurer.

Documentation

– Analyse de la société ISE, « Exploiting SOHO Routers » :
http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp

4 Rappel des avis émis

Dans la période du 26 avril au 02 mai 2013, le CERTA a émis les publications suivantes :

– CERTA-2013-AVI-276 : Vulnérabilité dans Citrix NetScaler Access Gateway Enterprise Edition
– CERTA-2013-AVI-277 : Multiples vulnérabilités dans VMware
– CERTA-2013-AVI-278 : Multiples vulnérabilités dans McAfee ePolicy Orchestrator
– CERTA-2013-AVI-279 : Vulnérabilité dans le système SCADA MatrikonOPC Security Gateway
– CERTA-2013-AVI-280 : Vulnérabilité dans le système SCADA MatrikonOPC A et E Historian
– CERTA-2013-AVI-281 : Vulnérabilité dans strongSwan
– CERTA-2013-AVI-282 : Vulnérabilité dans FreeBSD NFS Server
– CERTA-2013-AVI-283 : Multiples vulnérabilités dans MediaWiki
– CERTA-2013-AVI-284 : Vulnérabilité dans HP LaserJet

Gestion détaillée du document

26 avril 2013 version initiale.