Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 avril 2013
N° CERTA-2013-ACT-017

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-017

1 Exposition sur Internet d'interfaces séries d'équipements *via* des convertisseurs

Les interfaces d'administration dites "série" (RS-232, RS-485, etc.) sont utilisées depuis de nombreuses années pour accéder à des équipements. Souvent présentes dans les environnements industriels, on les retrouve également sur certains serveurs, généralement pour conserver un moyen d'administration en cas de problème réseau.

Les limitations intrinsèques de ces interfaces font qu'elles sont de plus en plus associées à des boîtiers de conversion qui permettent l'accès *via* un canal TCP/IP.

Ces boîtiers ne demandent généralement pas d'authentification avant d'accéder au port série et il suffit parfois de se connecter sur le port TCP associé pour pouvoir envoyer des commandes aux équipements connectés.

L'analyse récemment menée par un chercheur sur ce type de boîtiers lui a permis de découvrir plus de 13000 équipements connectés à Internet et ne nécessitant pas d'authentification. Certains permettaient d'obtenir directement une console privilégiée sur des serveurs de production.

Le CERTA recommande donc de recenser l'ensemble des équipements de ce type et de s'assurer de leur sécurisation en appliquant les mesures présentée dans l'article consacré aux systèmes industriel cité dans la section documentation.

Documentation

- Bulletin d'actualité numéro CERTA-2012-ACT-030, *Systèmes industriels et supervision par Internet* :
- Bulletin d'actualité CERTA-2012-ACT-030 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-030/

2 Mise en garde contre les variantes de Zeus

Le CERTA constate une utilisation toujours aussi active des logiciels malveillants dérivés du cheval de Troie "Zeus/Zbot". Son code source ayant été diffusé sur l'Internet, il est facile de le modifier et d'y ajouter de nouvelles fonctionnalités.

Ces nouvelles versions sont souvent repackagées/modifiées afin de ne plus être détectées par les antivirus. La principale fonctionnalité de ce logiciel est d'exfiltrer des données d'authentifications comme les identifiants bancaires, de messagerie, de serveur FTP, de réseaux sociaux etc.

Pour un réseau d'entreprise, les conséquences d'une telle compromission peuvent être importantes. Si un administrateur s'authentifie sur une machine infectée, il est alors possible pour l'attaquant de récupérer ses identifiants et de propager le malware sur toutes les machines où ces identifiants sont valides.

Le symptôme le plus courant permettant de détecter l'activité de ce type de logiciel malveillant, sur une machine infectée, est le doublement de certains caractères spéciaux tel que l'accent circonflexe lors de la saisie de texte. Afin de prévenir et limiter ce type de compromission, le CERTA recommande de :

1. sensibiliser les utilisateurs vis-à-vis des logiciels qu'ils téléchargent;
2. filtrer les pièces jointes en fonction de leur type sur les serveurs de messagerie, en prêtant une attention particulière aux fichiers exécutables;
3. avoir un mot de passe d'administrateur local différent pour chaque poste utilisateur.

3 Sortie d'une version de test de EMET 4.0

Le 18 avril 2013 *Microsoft* a publié la version 4.0 en béta de l'outil *EMET* (Enhanced Mitigation Experience Toolkit). Dans un précédent bulletin le CERTA avait présenté les principes fondamentaux de ce logiciel qui permet de prévenir certaines exploitations de failles applicatives. Cette nouvelle version ajoute et renforce plusieurs mécanismes de sécurité :

- renforcement du système de protection contre les exploitations de type *Return Oriented Programming* ;
- ajout d'une prévention contre les attaques de type « homme du milieu » (man in the middle) pour le protocole SSL/TLS ;
- amélioration de sa compatibilité avec des produits *Microsoft* répandus ;
- ajout d'une remontée des alertes (configurable) aux administrateurs et à *Microsoft* ;
- ajout d'un « audit mode » permettant de faciliter les tests de non-régression avant de déployer l'outil sur un parc.

La dernière version stable d'*EMET* est la version 3.0. *Microsoft* a planifié la publication stable de *EMET* 4.0 pour le 14 mai 2013. Dans l'intervalle, le CERTA ne recommande pas son intégration dans un système en production. Il peut cependant être pertinent de le déployer sur un environnement de test afin de commencer à qualifier son impact sur les applications métier.

Documentation

- Présentation d'EMET 4.0 sur le blog Security Research & Defense de Microsoft :
  `http://blogs.technet.com/b/srd/archive/2013/04/18/introducing-emet-v4-beta.aspx`
- Bulletin d'actualité CERTA-2012-ACT-016 du 20 avril 2012 :
  `http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-016/CERTA-2012-ACT-016.html`

4 Rappel des avis émis

Dans la période du 19 au 25 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-262 : Vulnérabilité dans Citrix XenServer
- CERTA-2013-AVI-263 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTA-2013-AVI-264 : Vulnérabilité dans Huawei Access Router
- CERTA-2013-AVI-265 : Vulnérabilité dans Huawei Versatile Security Manager
- CERTA-2013-AVI-266 : Vulnérabilité dans Xen
- CERTA-2013-AVI-267 : Multiples vulnérabilités dans Avaya Communication Manager
- CERTA-2013-AVI-268 : Multiples vulnérabilités dans ClamAV
- CERTA-2013-AVI-269 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTA-2013-AVI-270 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTA-2013-AVI-271 : Multiples vulnérabilités dans Citrix CloudPlatform
- CERTA-2013-AVI-272 : Multiples vulnérabilités dans Cisco NX-OS
- CERTA-2013-AVI-273 : Vulnérabilité dans F-Secure
- CERTA-2013-AVI-274 : Multiples vulnérabilités dans Cisco Device Manager
- CERTA-2013-AVI-275 : Multiples vulnérabilités dans Cisco Unified Computing System

Gestion détaillée du document

26 avril 2013 version initiale.