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 07 décembre 2015
N° CERTFR-2015-ACT-049

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-049

1 - Risques encourus et rappels sur les recommandations liés à l'utilisation des interfaces de gestion intelligente de matériel

En 2013, le CERT-FR alertait déjà sur les vulnérabilités présentes dans les interfaces de gestion intelligente de matériel. Pour rappel, ces interfaces offrent la possibilité de contrôler une machine physique à distance dès lors que celle-ci est alimentée en courant. Ces cartes, dédiées ou intégrées à la carte mère, embarquent un système d'exploitation minimal et autonome. Cependant celui-ci est bien souvent dépourvu de la moindre sécurité alors même qu'il est la porte d'entrée permettant d'accéder au contrôle total de la machine (matériel et logiciel). Le CERT-FR recommande la lecture du précédent bulletin d'actualité sur le sujet ainsi que d'un papier paru peu de temps après pour plus d'informations sur les vulnérabilités présentes sur ces systèmes. En 2015, force est de constater que la situation n'a quasiment pas évolué. L'objet du présent bulletin d'actualité est donc de rappeler les risques encourus ainsi que les recommandations d'usage.

Les risques en cas de compromission vont du déni de service (extinction pure et simple de la machine) jusqu'à la persistance d'une porte dérobée (survie à la réinstallation du système d'exploitation et du BIOS/UEFI) en passant par l'enregistrement des frappes clavier et captures d'écrans. Ces risques sont d'autant plus critiques que leur détection n'est absolument pas prévue par la plupart des solutions de sécurité. En effet, le système d'exploitation, le processeur et la mémoire de ces interfaces de gestion étant indépendants de ceux installés sur la machine, ils sont ainsi exclus de la surveillance effectuée par les logiciels de sécurité installés sur le système d'exploitation de la machine.

Concernant l'accès à ces interfaces, on distingue deux cas de figure :

- le premier consiste à utiliser un contrôleur réseau dédié présent sur la carte d'extension de l'interface de gestion à distance et donc invisible par le système d'exploitation de la machine ;
- le second consiste à utiliser un contrôleur réseau partagé qui recevra donc le trafic usuel du serveur ainsi que le trafic de l'interface de gestion à distance. Dans cette configuration, le contrôleur utilisera une sorte de multiplexage pour distinguer les deux trafics.

L'utilisation d'un contrôleur réseau partagé est déconseillée du point de vue de la sécurité. En effet, cela reviendrait à exposer sur un réseau qui n'est pas forcément de confiance une interface peu sécurisée et offrant un contrôle total sur la machine. Malheureusement, cette configuration est encore trop fréquemment rencontrée. Elle peut parfois s'expliquer par la méconnaissance de l'existence de ces interfaces ou de leur configuration, lorsque ce n'est pas à cause du choix assumé d'économiser l'utilisation d'un port réseau. Cette configuration aboutit généralement à la situation où l'interface de gestion se retrouve exposée sur internet, comme en témoignent certaines statistiques réalisées par Dan Farmer, un chercheur déjà à l'origine de plusieurs papiers sur le sujet.

À la lumière de ces informations, le CERT-FR recommande de ne pas utiliser les interfaces de gestion hors bande et de les désactiver explicitement sur les machines où elles sont installées. Toutefois, si leur utilisation est indispensable, il convient de considérer ces interfaces comme extrêmement sensibles en appliquant les principes de défense en profondeur dont les plus importants sont repris ici :

- utilisation d'un contrôleur réseau dédié ;

- connexion à un réseau d'administration dédié et déconnecté d'internet ;
- mise en place de politiques de filtrage sur le réseau d'administration ;
- modification des paramètres par défaut (utilisateur, mot de passe, configuration automatique de l'adresse IP, etc.).

Documentation

- Vulnérabilités présentes dans les interfaces de gestion intelligente de matériel :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-028/CERTA-2013-ACT-028.html
- Illuminating the Security Issues Surrounding Lights-Out Server Management :
  https://jhalderm.com/pub/papers/ipmi-woot13.pdf
- Sold Down the River :
  http://fish2.com/ipmi/river.pdf
- IPMI Security Best Practices :
  http://fish2.com/ipmi/bp.pdf

2 - Retour sur la conférence GreHack 2015

La troisième édition de la conférence GreHack, traitant de sécurité informatique, s'est déroulée à Grenoble le 20 novembre dernier.

Au cours de cette conférence réunissant de nombreux experts en sécurité des systèmes d'information, plusieurs sujets ont été abordés :

- Dans la présentation liminaire intitulée "Failure is not an option", Philippe Biondi est revenu sur les bogues logiciels et matériels qui ont marqué l'histoire. Il a ensuite proposé plusieurs méthodes à intégrer dans un cycle de développement logiciel qui permettent d'éliminer le maximum de bogues.
- La seconde présentation concernait les automates industriels SCADA. Une démonstration d'injection de code dans un PLC de type S7-300 a été réalisée.
- La présentation suivante détaillait comment détecter des anomalies au niveau des communications utilisant le protocole GOOSE. Ce protocole est utilisé pour transmettre des données sur des réseaux électriques. Plusieurs contraintes temps-réel empêchent d'implémenter des systèmes de sécurité comme la vérification d'intégrité et la confidentialité.
- Xavier Martin et Camille Mougey ont expliqué leur méthode basée sur l'apprentissage autonome et les algorithmes mégadonnées, pour mettre en évidence des anomalies dans des scans massifs d'adresses IPs.
- Ludovic Jacquin a montré en quoi l'utilisation de paquets ICMP trop petits ou trop grands pouvait mener à un déni de service lors de l'utilisation de certains types de tunnels.
- L'attaque "Logjam" a été présentée par Emmanuel Thomé, celle-ci permet de trouver certaines clés jetables générées par Diffie-Hellman notamment utilisé dans le protocole TLS. Les chercheurs ont remarqué que dans 92,3% des cas, seuls deux nombres premiers distincts sont utilisés pour générer le corps fini servant à faire les calculs. Ainsi, en faisant de nombreux pré-calculs sur ces deux nombres, il est possible de retrouver rapidement le logarithme discret utilisé dans Diffie-Hellman.
- Tobias Ruck et Miranda Mowbray ont proposé des méthodes basées sur des règles SQL pour détecter les codes malveillants qui utilisent des générateurs aléatoires de domaine.
- Dans sa présentation "Hacking a Sega Whitestar Pinball", Pierre Surply explique comment il a réussi à conduire la rétro-ingénierie d'un composant BSMT2000 DSP qui est utilisé dans le circuit audio d'un flipper.
- Dans la dernière présentation, intitulée « Draw me a Local Kernel Debugger », Samuel Chevet et Clément Rouault ont proposé une méthode pour implémenter un debogueur noyau local, c'est-à-dire un débogueur s'exécutant sur le même système que le noyau debogué. Leur debogueur interagit directement avec la bibliothèque de débogage de Windows (dbgeng.dll) et le pilote kldbgdrv.sys, comme le ferait WinDbg.

Documentation

- http://grehack.fr
- http://grehack.fr/data/grehack2015/slides/GreHack 2015 - Keynote - Failure is not an option.pdf
- http://grehack.fr/data/grehack2015/paper/Grehack 2015 - Paper - Industrial Control Systems Dynamic Code Injection.pdf
- http://grehack.fr/data/grehack2015/paper/Grehack 2015 - Paper - Corrupted GOOSE Detectors.pdf

- http://grehack.fr/data/grehack2015/slides/GreHack 2015 - Slides - Corrupted GOOSE Detectors.pptx
- http://grehack.fr/data/grehack2015/paper/Grehack 2015 - Paper - New Results for the PTB-PTS Attack.pdf
- http://grehack.fr/data/grehack2015/slides/GreHack 2015 - Slides - New results for the PTB-PTS attack.pdf
- http://grehack.fr/data/grehack2015/paper/Grehack 2015 - Paper - Linnea.pdf
- http://grehack.fr/data/grehack2015/slides/GreHack 2015 - Slides - Linnea.pdf
- http://grehack.fr/data/grehack2015/paper/Grehack 2015 - Paper - Hacking a Sega Whitestar Pinball.pdf
- http://grehack.fr/data/grehack2015/slides/GreHack 2015 - Slides - Linnea.pdf
- http://grehack.fr/data/grehack2015/paper/Grehack 2015 - Paper - Hacking a Sega Whitestar Pinball.pdf
- http://grehack.fr/data/grehack2015/slides/GreHack 2015 - Slides - Hacking a sega whitestar pinball.pdf
- http://grehack.fr/data/grehack2015/slides/Grehack 2015 - Invited talk - Draw me A Local Kernel Debugger.pdf

3 - Rappel des avis émis

Dans la période du 30 novembre au 06 décembre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-508 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2015-AVI-509 : Vulnérabilité dans redmine
- CERTFR-2015-AVI-510 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-511 : Vulnérabilité dans Xen
- CERTFR-2015-AVI-512 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2015-AVI-513 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2015-AVI-514 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-515 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-516 : Multiples vulnérabilités dans Huawei LogCenter
- CERTFR-2015-AVI-517 : Multiples vulnérabilités dans OpenSSL
- CERTFR-2015-AVI-518 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

07 décembre 2015 version initiale.