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 03 avril 2017
N° CERTFR-2017-ACT-014

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-014

1 - Intelligent Platform Management Interface (IPMI)

Introduction

L'IPMI (Intelligent Platform Management Interface, première version en 1998 puis seconde version en 2004) est un ensemble de spécifications pour un système informatique autonome offrant des fonctionnalités hors bande de gestion et de supervision indépendamment du système d'exploitation de l'hôte, de son CPU, BIOS, etc. Cette IPMI est implémentée dans le BMC (Baseboard Management Controller), un microcontrôleur intégré à la carte mère du serveur ou sur une carte fille qui possède son propre stockage et son propre système d'exploitation (par exemple Linux 2.6.X sur les BMC supermicro en 2013 et quelques Mo de stockage [1]).

Les IPMI sont devenues une fonctionnalité standard dans les serveurs aujourd'hui. On trouve différentes implémentations/produits chez les constructeurs à savoir iDRAC chez Dell, iLO chez HP, Remote Supervisor Adapter chez IBM et MegaRAC pour ASUS, Tyan, Intel et Supermicro (entre autres). [2]

Utilité

L'IPMI propose les fonctionnalités suivantes :

- une interface web d'administration ;
- virtual console : permet de disposer d'une interface KVM (Keyboard-Video-Mouse) à distance ;
- virtual media : permet de monter un média virtuel ou physique à distance sur le serveur et le démarrer ;
- mise à jour du micrologiciel des microcontrôleurs présents sur le système ;
- gestion de l'alimentation (extinction, allumage, redémarrage du serveur) ;
- supervision des tensions, températures, vitesses de ventilateurs, etc.

Du fait de sa complète séparation vis-à-vis du CPU, BIOS, OS (etc.) de la machine hôte et de sa carte réseau dédiée, l'IPMI offre des fonctionnalités clés. Elle permet en effet d'administrer et de superviser le serveur :

- avant que le système d'exploitation ne soit démarré, on peut donc configurer le BIOS par ce biais ;
- quand le serveur est éteint (possibilité de le démarrer à distance) ;
- après un crash du système d'exploitation ou matériel (permet de visualiser la raison du crash via le KVM).

Configuration et sécurité

Un tel composant doit être connecté en hors bande via sa carte réseau dédiée afin de ne pas exposer ses fonctionnalités. Toutefois, si cette carte réseau dédiée est enlevée, l'IPMI partage un des ports réseau de la carte mère.

L'IPMI comporte 3 rôles différents afin de segmenter et limiter les accès utilisateurs :

- le rôle utilisateur qui n'a qu'un accès en lecture aux informations de supervision du système et ne peut effectuer aucune action de gestion ni accéder aux informations sensibles ;

– le rôle opérateur est utile lors d'un crash (ex. : une interruption non masquable qui génère une copie mémoire), car il peut récupérer les informations de diagnostics et redémarrer la machine ;
– le rôle administrateur permet de configurer l'IPMI lors de la première installation du serveur.

Une des bonnes pratiques est d'utiliser un serveur LDAP/RADIUS avec SSL pour gérer les utilisateurs, les droits, désactiver les rôles opérateur et administrateur afin de les activer au besoin par l'administrateur LDAP/RADIUS. L'attribution des rôles doit être fine et judicieuse afin d'éviter que tous les utilisateurs ne soient administrateurs. Il convient également de sécuriser l'accès WEB à la console d'administration en chiffrant la connexion HTTP et en réduisant l'accès à cette dernière via des listes de contrôle d'accès ou des pare-feu.

Dangers induits

De par leur nature et leur configuration par défaut, les implémentations d'IPMI réalisées par les constructeurs constituent des failles de sécurité non négligeables. La première bonne pratique consiste à mettre celles-ci sur un réseau d'administration séparé d'internet, au moins logiquement (ex : vlan), ou au mieux physiquement avec des équipements réseau dédiés. Via des scans d'internet [1], on constate plus de 100 000 IPMIs exposées avec 40 % d'entre elles potentiellement vulnérables à distance. Si l'IPMI est détournée par des attaquants, elle constituera une porte dérobée de premier choix, car celui-ci aura un contrôle quasi total sur la machine.

La plupart des serveurs ont une configuration d'usine avec les IPMIs activées, accessibles via la carte réseau dédiée ou en partageant la carte réseau de la carte mère. Elles récupèrent une IP dynamiquement ce qui les rend directement accessibles sans intervention humaine. L'IPMI fonctionnant même lorsque le serveur est éteint, le risque que son accès web soit exposé publiquement en est augmenté sensiblement. Les constructeurs livrent leur matériel avec des identifiants de connexion par défaut.

Les spécifications IPMI indiquent de stocker les mots de passe en clair sur le BMC, ce qui rend le stockage non sûr et peut aboutir à la compromission de tout le parc de serveurs si le même mot de passe est réutilisé. La nature et les fonctionnalités de l'IPMI permettent un certain nombre d'attaques réalisables avec une IPMI compromis (par mot de passe par défaut, exploitation de vulnérabilités). Les fonctionnalités de virtual média et de virtual console implémentée dans la plupart des IPMIs permettent à un attaquant d'avoir quasiment autant de capacités que s'il accédait physiquement à la machine. Ce dernier pourrait modifier la configuration BIOS, démarrer sur un autre système et exfiltrer les données.

Il est possible d'insérer un logiciel espion au sein même de l'IPMI, car celle-ci possède un système d'exploitation. Détecter un tel logiciel espion est difficile, car celui-ci est inséré à un niveau très bas. Il serait persistant, survivrait à une réinstallation de l'OS voire un changement des disques durs du serveur. L'IPMI étant accessible depuis le système hôte du serveur via certains outils, il est possible de flasher son micrologiciel via le système d'exploitation hôte (après une compromission de l'OS hôte).

Conclusion

Les IPMIs ouvrent de nombreuses perspectives pour la gestion et la supervision de parc ainsi que la reprise d'activité. Celles-ci peuvent permettre de réduire les délais d'interruption de service et de respecter plus facilement le SLA (Service Level Agreement ou accord de niveau de service).

On remarque que même si d'importantes failles ont été trouvées les années précédentes, on en trouve encore d'importantes aujourd'hui. Il est donc nécessaire d'utiliser ces équipements en environnement maitrisé et sécurisé, mais aussi d'utiliser une implémentation rigoureuse en termes de sécurité.

Il est à la charge de l'utilisateur de mettre son IPMI sur un réseau séparé d'internet et de mettre à jour aussi régulièrement que possible le micrologiciel afin de réduire au maximum les risques. Et bien évidemment, si l'utilisation de l'IPMI n'est pas indispensable, il est fortement recommandé de le désactiver.

Sources

– https://www.usenix.org/system/files/conference/woot13/woot13-bonkoski_0.pdf
– https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface
– http://www.cvedetails.com/product/23648/HP-Integrated-Lights-out-4-Firmware.html?vendor_id=10
– https://www.usenix.org/conference/woot13/workshop-program/presentation/bonkoski
– http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-028/CERTA-2013-ACT-028.html

2 - Retours sur la conférence *CanSecWest* et le concours *Pwn2Own*

Contexte

La conférence *CanSecWest* est une conférence portant sur les différentes thématiques de la sécurité numérique appliquée, se déroulant à *Vancouver*. L'édition 2017 de cette conférence a abordé plusieurs aspects, aussi bien du côté matériel et bas niveau que d'un point de vue plus global sur la sécurisation des systèmes. Par ailleurs, cette conférence héberge depuis 10 ans le concours *Pwn2Own*, incitant les chercheurs en sécurité à démontrer la faisabilité d'attaques sur des plateformes modernes pour les divulguer à l'éditeur et les corriger.

Conférences thématiques

Mercredi

Différentes techniques et problématiques ont été présentées le premier jour de la conférence. En particulier, la conférence d'ouverture, bien que très centrée sur les États-Unis, mettait en exergue les différences entre les certifications de conformité réglementaire que peuvent obtenir une entité et leur niveau de sécurité réelle.

De même, différentes techniques d'exploitation ont été présentées, telles que la chaîne de vulnérabilités utilisée pour compromettre un téléphone *Nexus* lors d'un concours de sécurité, des techniques permettant d'effectuer un massage précis du tas dans le noyau *iOS*, ainsi que l'utilisation des fonctionnalités de trace processeur sur la plateforme *Intel* pour améliorer la couverture de code lors d'un frelatage de donné es (fuzzing).

Par ailleurs, une étude sur différents systèmes embarqués a été présentée afin d'illustrer le manque de prise en compte de la sécurité dans les chaînes de démarrage sécurisées sur des objets connectés. Enfin, des outils permettant d'améliorer la compréhension de code *PowerShell* ou d'effectuer des analyses de captures mémoires par introspection de machine virtuelle ont été présentés.

Jeudi

Deux présentations étaient centrées sur les attaques par radiofréquences, une illustrant les déficiences de blindage de certains équipements informatiques face à une radio courte portée, et l'autre illustrant la prise de contrôle d'un drone à l'aide d'une radio logicielle, après avoir effectué la rétro-ingénierie du protocole radio.

Deux présentations se focalisaient sur la sécurité automobile, présentant une plateforme de visualisation des messages d'un bus `CAN` et une solution de détection d'anomalies basée sur un système d'apprentissage.

Une attaque de bas niveau a été présentée dans la fonctionnalité d'ajout de processeur à chaud sur un serveur. Cette attaque démontrait la faisabilité d'injection de code en espace mémoire surprivilégié via une injection en mémoire par accès direct.

Par ailleurs, une présentation s'est focalisée sur la sécurité des machines à voter, montrant qu'un défaut de prise en compte de la sécurité, mais également un manque de tests lors du développement de ces machines peut poser des problèmes graves.

Enfin, le cadriciel *Chipsec*, développé par *Intel*, a été présenté. Ce cadriciel permet d'effectuer des tests de sécurité sur différentes fonctionnalités fournies par le microgiciel embarqué.

Vendredi

Une équipe de *Microsoft* a présenté les dernières contre-mesures utilisées dans la dernière version de *Windows 10*. Ces différentes contre-mesures visent à éliminer des catégories complètes de vulnérabilités, et à renforcer la difficulté d'exploitation sur les différentes parties du système *Windows*. Ces mesures d'atténuation concernent la vérification de signature de tout code exécuté, la préservation de l'intégrité du flot de contrôle en vérifiant la légitimité des appels effectués par un programme, ainsi que la protection des adresses de retour, qui a été désactivée suite à la découverte en interne d'un bogue critique. De même, la protection du noyau par un système de virtualisation a été abordée. Par ailleurs, plusieurs études de sécurité ont été présentées sur les hyperviseurs *VMWare*, *Qemu* et le sous-système graphique de *Windows*.

Concours *Pwn2Own*

Le concours *Pwn2Own* est un concours organisé par le programme *Zero Day Initiative* de la société *Trend Micro*, qui fournit des prix (*bounties*) aux chercheurs démontrant une vulnérabilité dans un système et donnant cette vulnérabilité au constructeur pour correction. Le concours se concentrait cette année sur 5 domaines spécifiques,

à savoir des systèmes serveurs, des applications de bureautique telles que *Microsoft Of fice* et *Adobe Reader*, les navigateurs, les élévations de privilèges sur *Ubuntu*, *Apple Mac OS* et *Microsoft Windows*, et enfin les échappements de machine virtuelle. Les différents participants au concours ont pu réaliser des démonstrations de chaînes complètes permettant d'aller de la compromission d'un navigateur jusqu'à l'exécution de code sur l'hyperviseur de la machine concernée. Ce concours a permis, cette année, de remonter plus de 50 vulnérabilités aux éditeurs.

Conclusion

Le CERT-FR recommande de prendre en compte les avancées techniques dans le domaine de la sécurité afin d'améliorer la résilience des systèmes informatiques face aux techniques d'attaques toujours plus évoluées. De même, le CERT-FR recommande de mettre à jour les systèmes informatiques vers les dernières versions des logiciels disponibles pour bénéficier des correctifs de sécurité et des fonctionnalités d'atténuation de surface d'attaque.

Documentation

- https://www.slideshare.net/CanSecWest
- https://cansecwest.com/agenda.html
- https://shanek2.github.io/inVtero.net/
- https://github.com/chipsec/chipsec
- http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ACT-006/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ACT-009/index.html

3 - Rappel des avis émis

Dans la période du 27 mars au 02 avril 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-ALE-006 : Multiples vulnérabilités dans SCADA Siemens RUGGEDCOM ROX I
- CERTFR-2017-AVI-092 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2017-AVI-093 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2017-AVI-094 : Vulnérabilité dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-095 : Multiples vulnérabilités dans Google Chrome et Chrome OS
- CERTFR-2017-AVI-096 : Multiples vulnérabilités dans SCADA Wonderware by Schneider Electric InTouch Access Anywhere
- CERTFR-2017-AVI-097 : Multiples vulnérabilités dans SUSE

Gestion détaillée du document

03 avril 2017 version initiale.