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 18 avril 2016
N° CERTFR-2016-ACT-016

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-016

1 - Vulnérabilité Flash Player CVE-2016-1019

Le 6 avril, Adobe publie un bulletin de sécurité concernant une vulnérabilité exploitée dans la nature, identifiée CVE-2016-1019 [1]. Cette vulnérabilité peut permettre une exécution de code arbitraire via une corruption mémoire impactant les versions du logiciel Flash Player 20.0.0.306 et antérieures, pour les systèmes Windows, Linux et Mac. Corrigée le 7 avril par Adobe [2][4] dans la version 21.0.0.197 de Flash Player, elle est cependant intégrée aux kits d'exploitation `Magnitude` et `Angler`. La mitigation introduite dans la version 21.0.0.213 de Flash, isolant les objets de type `ByteArray` en les stockant sur un tas isolé, permet de bloquer l'exploitation de cette vulnérabilité.

L'analyse de cette vulnérabilité révèle l'utilisation de deux fichiers Flash SWF. Le premier fichier est compilé en ActionScript 3 tandis que le second est compilé en ActionScript 2 via l'utilisation du compilateur open source MTASC. Pour communiquer entre eux, une connexion est instanciée via un objet de type `LocalConnection`.

Pour déclencher la corruption mémoire, des messages vont transiter entre ces deux fichiers de manière à appeler des fonctions de callback. Le premier fichier crée la connexion, puis déclare ses fonctions callback `start` et `end`. Il reste ensuite en attente de connexion.

```
var_34 = new LocalConnection();
[...]var_34.client = { start:function()~: * //start { class_14.method_34(); }, end:funct
```

Lorsque le second fichier SWF est chargé en mémoire, la fonction `send` est utilisée pour appeler la fonction de callback `start` précédemment déclarée dans le fichier principal.

```
Main._lc.send("toAS3" + Main._lcId,"start");
```

La fonction `start` utilise des objets de type `ConvolutionFilter` afin de procéder à un massage du tas. L'utilisation de ce type d'objet sort de l'ordinaire : habituellement, des objets de type `Vector` ou `ByteArray` sont utilisés. Leur utilisation peut s'expliquer par la présence de code compilé en ActionScript 2, les objets `Vector` et `ByteArray` n'étant pas implémentés en ActionScript 2. De plus, la propriété `Matrix` d'un objet `ConvolutionFilter` est un bon candidat pour contrôler le tas, et son utilisation permet de contourner la mitigation déplaçant les objets `Vector` sur un tas isolé.

```
while(loc2 < loc1) //_loc1_ = 596 [0x254]{
var_35[_loc2_] = new ConvolutionFilter(0,1);
_loc2_++;
}
```

Le second fichier SWF est ensuite contacté pour déclencher un appel à sa fonction de callback. Plusieurs opérations sont effectuées au sein de cette fonction : d'après l'article de la société FireEye [3], la corruption mémoire est provoquée par l'appel à une fonction native de la machine virtuelle ActionScript 2. Les valeurs `2204` et `200` semblent correspondre au constructeur de l'objet `FileReference`.

```
global.ASnative(2204,200).call(Main._tf);
```

Une fois l'exécution de cette fonction terminée, le flot d'exécution est rendu au fichier SWF principal via un appel à la fonction de callback `end`.

```
Main._lc.send("toAS3" + Main._lcId,"end");
```

C'est cette fonction qui va vérifier si la taille d'un objet `ByteArray` a été correctement corrompue.

```
loc1 = var_29.length; //ByteArray
if(loc1 != 4.294967295E9) //'0xffffffff' {
method_27("");
}
[...]
if(var_43) {
class_15.Exec();
}
```

Une fois l'objet `ByteArray` contrôlé par l'attaquant, celui-ci utilise des routines de lecture et d'écriture afin de contourner les protections ASLR et DEP.

```
static function method_26(param1:uint)~: uint {
if(param1 = 3.221225472E9) {
method_27("");
}
var_29.position = param1;
return var_29.readUnsignedInt();
}
static function method_29(param1:uint, param2:uint)~: * {
if(param1 = 3.221225472E9) {
method_27("");
}
var_29.position = param1;
var_29.writeUnsignedInt(param2);
}
```

Le CERT-FR recommande fortement d'utiliser la dernière version du logiciel Flash Player de manière à bénéficier des dernières mitigations ainsi que des correctifs disponibles.

Documentation

- [1] https://helpx.adobe.com/security/products/flash-player/apsa16-01.html
- [2] https://helpx.adobe.com/security/products/flash-player/apsb16-10.html
- [3] https://www.fireeye.com/blog/threat-research/2016/04/cve-2016-1019_a_new.html
- [4] http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-116/index.html

2 - Rançongiciels : état des lieux

Depuis plusieurs mois, le CERT-FR a pu constater au niveau national, un accroissement significatif des campagnes de pourriels, vecteurs de rançongiciels.

Un rançongiciel est un programme malveillant dont l'objectif est de chiffrer partiellement ou entièrement les données sur le système cible. En fonction des privilèges d'exécution et des mesures de sécurité du poste, le programme malveillant chiffre les données de la session de l'utilisateur, les fichiers partagés via les lecteurs réseau, voire les données du système. L'objectif est de proposer à la victime de récupérer ses données en l'échange du paiement d'une rançon.

Vecteurs identifiés

Les rançongiciels analysés jusqu'à présent n'ont pas montré de mécanismes de déplacements latéraux : le pourriel reste le vecteur principal de diffusion même si quelques signalements reçus par le CERT-FR font état de compromissions à partir d'une simple consultation de site Internet.

Plus récemment, le CERT-FR a constaté que des rançongiciels sont envoyés par un pourriel à quelques personnes bien ciblées (cadres de l'organisme) : dans ce cas, le contenu du courrier est adapté à la cible afin de faciliter l'exécution du code malveillant.

Logique d'infection principalement constatée

Le mode opératoire le plus souvent constaté par le CERT-FR est le suivant :

1. réception d'un pourriel contenant une pièce jointe (ZIP, RAR, SRC, CAB,) ;
2. action volontaire de l'utilisateur qui ouvre la pièce jointe ;
3. décompression éventuelle du fichier joint ;
4. ouverture du document (document Office contenant des macros, script JS ou Powershell brouillé, fichiers .src ...) ;
5. exécution du code qui provoque soit le chiffrement, soit le téléchargement de la charge malveillante depuis diverses sources possibles (TOR, serveurs ou ordinateurs compromis, service de stockage de fichier en nuage, ...) ;
6. exécution de la charge malveillante ;
7. début du chiffrement soit immédiatement, soit après redémarrage provoqué par la charge malveillante.

Dans la plupart des cas, les environnements Windows sont la cible de ces attaques, mais d'autres systèmes d'exploitation peuvent être victimes d'un mode opératoire similaire.

Rappel des bonnes pratiques

Ces bonnes pratiques ne sont pas exhaustives, mais constituent un recueil générique des orientations permettant de réduire au maximum l'infection initiale par un rançongiciel ainsi que la portée des actions de chiffrement.

- Vérifier les autorisations d'accès aux ressources partagées (ACL sur le partage et sur le système de fichiers) : notamment, les ressources accessibles en écriture doivent être limitées aux seuls utilisateurs qui en ont le besoin fonctionnel ;
- Appliquer le principe du moindre privilège, en attribuant aux différents comptes les seuls privilèges qui leur sont strictement nécessaires dans l'exécution de leurs tâches : dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou naviguer sur Internet ;
- Mettre en oeuvre une politique de filtrage des passerelles de messagerie (filtrage CAB, JS, EXE, etc.) ;
- Installer un antivirus sur les postes clients afin de se prémunir contre le téléchargement d'un code malveillant connu. Un antivirus adapté aux passerelles de messagerie peut permettre d'éliminer en amont les pourriels détectés malveillants. Par ailleurs, et dans le cas où la variante du rançongiciel n'est pas détectée, il convient d'envoyer dès que possible un échantillon du code malveillant aux éditeurs des solutions déployées ;
- Maintenir à jour les composants systèmes et applicatifs : la mise à jour régulière des systèmes d'exploitation et des applications présentes, demeure une action fondamentale, sans oublier les navigateurs, briques Java, Adobe Flash Player, suites bureautiques, etc. A noter que les versions obsolètes doivent être remplacées en priorité ;
- Ne pas activer les macros pour les documents Office. Microsoft a volontairement désactivé l'auto-exécution de ces macros depuis plusieurs années : même si l'ouverture d'un document vous incite à réactiver celles-ci, ne le faites pas, surtout lorsque l'origine est douteuse. Lorsque ces macros sont nécessaires pour certains documents, le centre de sécurité Microsoft Office permet d'activer celles-ci uniquement pour les documents chargés depuis une liste d'emplacements spécifiés ;
- Implémenter les stratégies de restrictions logicielles : SRP pour Windows XP et AppLocker pour Windows Vista et supérieur, ces stratégies visent à empêcher l'exécution de code à partir d'une liste noire de répertoires prédéfinis. Aussi, et lors de leur implémentation, il est important de vérifier que le service "Application Identity" (AppIDSvc) soit paramétré en démarrage automatique sur l'ensemble des postes pour que les restrictions logicielles soient opérantes (ce mode de démarrage peut être paramétré à travers une stratégie de groupe sur un domaine Windows). Si des dysfonctionnements sont rencontrés suite au déploiement de ces règles de blocage, il est nécessaire d'identifier les applications légitimes situées dans ces répertoires, et de

définir des règles en liste blanche afin d'autoriser leur exécution. Plus d'informations sont disponibles dans la section documentation (1) ;

- Sauvegarder les systèmes ainsi que les données : composante majeure dans le cadre de la reprise d'activité, les sauvegardes doivent être effectuées régulièrement sur un périmètre adapté (en priorité sur les serveurs hébergeant des données critiques), et stockées sur des médias tiers et isolés du réseau de production. La politique de sauvegarde doit également être adaptée, de telle sorte que les sauvegardes antérieures ne soient pas simplement écrasées, la sauvegarde la plus récente pouvant contenir une version chiffrée des données ;
- Éprouver le processus de restauration : dans le cas où la prestation de sauvegarde/restauration est externalisée, il convient de s'assurer que les points de contact sont clairement identifiés ; des tests réguliers doivent être menés afin de valider l'intégrité des données restaurées. De plus amples informations sont disponibles dans la section documentation (2) ;
- Bloquer les adresses utilisées par le code malveillant : après analyse d'échantillons, le CERT-FR peut décider d'établir des listes d'adresses ou URL utilisées par le rançongiciel identifié. Ces listes (définies pour des variantes précises - et très nombreuses) doivent idéalement alimenter les solutions de filtrages présentes au sein du SI (pare-feu, Proxy, ...), afin d'empêcher les communications lors d'échanges de clefs cryptographiques, ou simplement lors du téléchargement de la charge. A retenir : il n'est pas nécessaire de transmettre systématiquement les échantillons au CERT-FR, celui-ci se chargera de vous solliciter en cas de besoin.
- Sensibilisation des utilisateurs : Le CERT-FR recommande de sensibiliser régulièrement les utilisateurs face aux risques associés aux messages électroniques. Il convient en effet de ne pas cliquer sans vérification sur les liens ou ouvrir les pièces jointes présentes ; une attention toute particulière devant être apportée aux messages de provenance inconnue, l'apparence inhabituelle ou frauduleuse. L'expérience montre également qu'un exemple de courriels issus d'une campagne en cours est plus efficace qu'une sensibilisation "générique".

Réflexes en cas de détection de compromission

- Si des fichiers chiffrés sont découverts sur vos systèmes (ou plus généralement en cas de comportement anormal), le CERT-FR recommande de positionner les permissions des dossiers partagés en LECTURE SEULE afin d'empêcher le chiffrement des fichiers sur ceux-ci : les personnels pourront ainsi continuer de travailler localement et mettre à jour ultérieurement le partage ;
- le CERT-FR recommande de déconnecter immédiatement du réseau les machines identifiées, l'objectif est ici de bloquer la poursuite du chiffrement des documents ;
- Prendre contact immédiatement avec la chaîne de sécurité informatique de votre entité, afin de signaler l'incident (service informatique, RSSI, DSI);
- Le CERT-FR recommande de déposer plainte : dans ce cadre, il est nécessaire de réunir toutes les traces et indices qui pourraient servir comme éléments de preuve :
  - copies physiques des disques durs (ou VM) des postes compromis (il est important de conserver les dates de modifications des fichiers) ;
  - copies des journaux d'événements disponibles sur tout équipement réseau qui auraient pu permettre la communication des codes malveillants (proxy, pare-feu, etc.), en conservant leur format d'origine et concernant la période estimée de compromission.
- Afin de prévenir toute nouvelle compromission sur le même site, le CERT-FR recommande également de bloquer les communications avec le(s) serveur(s) mandataire(s): l'accès aux domaines, IP ou URLs identifiés dans le message malveillant.
- Côté serveur de messagerie : après identification du pourriel, le CERT-FR recommande de rechercher et supprimer les copies qui n'ont pas encore été distribuées dans les boîtes de messagerie des utilisateurs.
- Après éradication : le CERT-FR recommande la réinstallation complète du poste avec les dernières mises à jour (OS et applicatives) et enfin, la restauration d'une sauvegarde réputée saine des données de l'utilisateur. De plus, et dans le cadre de l'utilisation de profils itinérants, il convient de supprimer la copie serveur du profil afin de prévenir l'éventuelle répétition d'exécution des codes malveillants par ce biais.
- Le CERT-FR recommande de ne pas payer la rançon : en effet, le paiement ne garantit pas le déchiffrement des données et compromettra le moyen de paiement utilisé (notamment carte bancaire).

Enfin, les fichiers chiffrés peuvent être conservés par la victime au cas où, dans le futur, un moyen de recouvrement des données originales serait découvert. Sur ce point, bien que le déchiffrement de certaines souches ait pu être réalisé, cela reste cependant à ce jour exceptionnel et de moins en moins fréquent les attaquants améliorant constamment leurs cryptosystèmes.

Vecteurs d'infection

Les rançoncigiels sont distribués de différentes manières suivant les attaquants ou les campagnes. Nous présentons dans cette partie quelques exemples, mais il est important de noter que la liste n'est pas exhaustive et que les méthodes sont constamment en évolution.

Le vecteur initial est, le plus souvent, la réception d'un message électronique dont le contenu incite à l'ouverture d'une pièce jointe. Le type de fichier en pièce jointe peut être très varié, mais son ouverture mène, directement ou indirectement, au téléchargement et à l'exécution automatique de la charge qu'est le rançongiciel. Voici quelques exemples d'extensions de fichier pouvant être trouvées en pièce jointe :

- .exe : un fichier exécutable, de moins en moins utilisé, car souvent bloqué ;
- .doc : un document Microsoft Office, deux scénarios connus :
  - une macro malveillante est présente dans le document. Dans les versions récentes d'Office, leur exécution est désactivée par défaut, mais peut être activée manuellement par l'utilisateur. Pour cette raison, les attaquants ajoutent des éléments dans le pourriel afin d'inciter l'utilisateur à les activer,
  - le document est spécialement conçu pour exploiter une vulnérabilité à son ouverture et exécuter du code arbitraire ;
- .js : un fichier contenant du code JavaScript exécuté automatiquement à son ouverture ;
- .pdf.exe : un fichier exécutable (.exe) nommé spécialement pour faire croire à l'utilisateur que c'est un document PDF. Sous Windows, les extensions connues sont, par défaut, cachées. `Document.pdf.exe` sera par exemple affiché sous le nom `Document.pdf` dans l'explorateur Windows ;
- .zip, .rar ou .cab : une archive contenant d'autres fichiers, ajoutant un niveau d'indirection.

Il arrive également que des rançongiciels soient distribués par des kits d'exploitation, il est donc essentiel d'appliquer régulièrement les mises à jour de sécurité des logiciels.

Mise en garde contre les "vaccins"

Afin de lutter contre les rançongiciels, il apparaît de plus en plus fréquemment des antidotes (ou vaccins) disponibles sur Internet afin de bloquer spécifiquement une infection (modification d'une ACL, création d'une clé de la base de registre, etc.). Derrière ces astuces, qui peuvent être perçues comme une première surcouche de défense, il faut noter que les rançongiciels évoluent très rapidement : un vaccin peut être rapidement inefficace si un code malveillant évolue. Il convient donc d'être conscient du sentiment de sécurité éphémère que peuvent induire ces solutions. Le temps passé pour déployer ce type de solution peut être mis à profit pour mener d'autres actions de sécurité plus durables (AppLocker, mise à jour, etc.).

Si l'idée de vaccin spécifique à un code malveillant est assez ancienne, elle reste une méthode provisoire de sécurité efficace pour endiguer la propagation effective d'un ver informatique (cas de moins en moins fréquent) sur un réseau.

Documentation

- (1) Stratégies de restriction logicielle
  http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf
- (2) Guide des bonnes pratiques de l'informatique
  http://www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf
- (3) Mesures de prévention relatives à la messagerie
  http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

3 - Mise à jour mensuelle de Microsoft

Le 12 avril, lors de sa mise à jour mensuelle, Microsoft a publié treize bulletins de sécurité, dont six considérés critiques et sept importants :

- MS16-037 (critique) concernant Internet Explorer ;
- MS16-038 (critique) concernant le navigateur Edge ;
- MS16-039 (critique) concernant le composant Windows Graphics ;
- MS16-040 (critique) concernant Microsoft XML Core Services ;
- MS16-042 (critique) concernant Microsoft Office ;
- MS16-050 (critique) concernant Adobe Flash Player ;

– MS16-041 (important) concernant le cadriciel .NET ;
– MS16-044 (important) concernant Windows OLE ;
– MS16-045 (important) concernant Windows Hyper-V ;
– MS16-046 (important) concernant le service d'ouverture de session secondaire de Windows ;
– MS16-047 (important) concernant les protocoles distants SAM et LSAD ;
– MS16-048 (important) concernant CSRSS ;
– MS16-049 (important) concernant HTTP.sys.

Navigateurs

Cette mise à jour corrige six vulnérabilités dans Internet Explorer, dont cinq permettent une exécution de code à distance. Celles-ci sont considérées critiques dans le contexte de clients Windows (les versions serveur étant moins impactées). Pour empêcher l'exploitation de cinq de ces vulnérabilités, Microsoft a changé la manière dont Internet Explorer traite les objets en mémoire. La sixième vulnérabilité, CVE-2016-0162, pouvait déboucher sur une fuite d'informations. En effet, un attaquant pouvait exploiter une faille dans la manière dont Internet Explorer traitait les scripts JavaScript, lui donnant ainsi un accès en lecture sur certains fichiers de la machine victime.

Le greffon Adobe Flash Player d'Internet Explorer a également fait l'objet d'un correctif concernant une dizaine de vulnérabilités. Cela concerne notamment la CVE-2016-1019, ciblée par les kits d'exploitation Magnitude et Nuclear et qui a fait l'objet d'une alerte : CERTFR-2016-ALE-002.

Le navigateur Edge est également concerné par les vulnérabilités portant sur le greffon Adobe Flash Player.

De plus, il est touché par six autres vulnérabilités. Quatre vulnérabilités sont considérées critiques, une mauvaise gestion des objets en mémoire permettant une exécution de code à distance.

Les deux dernières vulnérabilités permettent un élévation de privilège. La vulnérabilité CVE-2016-0158 est liée à une mauvaise application des stratégies inter-domaines par Edge. La vulnérabilité CVE-2016-0161 permet une exécution d'un script avec un niveau de privilège équivalent à celui de l'utilisateur actuel, dans certaines conditions spécifiques.

Bureautique

Quatre vulnérabilités de type corruption de mémoire ont été corrigées dans Microsoft Office.

Celles-ci sont susceptibles de permettre une exécution de code à distance lors de l'ouverture d'un fichier spécialement conçu. Cependant, seule l'une d'entre elles est considérée critique, les autres étant jugées importantes car plus difficiles à exploiter.

A noter qu'Office est aussi concerné par l'une des failles du composant Windows Graphics. La vulnérabilité CVE-2016-0145 permet une exécution de code à distance lors de l'ouverture d'un document contenant des polices incorporées spécialement conçues. Dans le contexte de la suite bureautique, cette vulnérabilité est jugée importante.

Windows

Toutefois, dans le contexte de Windows, la vulnérabilité de corruption de mémoire CVE-2016-0145 est jugée critique. Les trois autres vulnérabilités affectant le composant Windows Graphics (CVE-2016-0143, CVE-2016-0165, et CVE-2016-0167) permettent une élévation de privilège en mode noyau, suite à un problème de gestion des objets en mémoire par Win32k . Microsoft rapporte que les vulnérabilités CVE-2016-0165 et CVE-2016-0167 ont été activement exploitées préalablement à la disponibilité de cette mise à jour.

La vulnérabilité CVE-2016-0147 touche l'analyseur de Microsoft XML Core Services 3.0 (MSCXML). Elle permet d'exécuter du code à distance si l'utilisateur se rend sur un site Internet spécialement conçu. Celle-ci est causée par un mauvais traitement des données utilisateur. Son niveau est considéré important. La vulnérabilité CVE-2016-0153 concerne Windows OLE pour un impact et un niveau équivalent.

Trois vulnérabilités importantes touchent le moteur de virtualisation Hyper-V de Windows. Les deux premières (CVE-2016-0089 et CVE-2016-0090) peuvent déboucher sur une fuite d'informations du système hôte, si un attaquant arrive à faire tourner une application malveillante dans le système invité. La troisième (CVE-2016-0088) peut permettre de sortir de la machine virtuelle et exécuter du code sur la machine hôte.

La vulnérabilité CVE-2016-0135 touche le service d'ouverture de session secondaire de Windows 10 et peut permettre une élévation de privilège avec les droits administrateur. Le Client-Server Run-time Susbsystem (CSRSS)

ne gère pas toujours correctement les jetons dans la mémoire, ce qui peut entraîner un contournement de sa fonctionnalité de sécurité. Cela permet à un attaquant, authentifié mais de faible privilège, d'exécuter du code en tant qu'administrateur.

En outre, le service HTTP.sys, qui gère la pile protocolaire HTTP 2.0, peut être mis à mal par des requêtes malveillantes, exposant le système à un déni de service.

Le cadriciel .NET est vulnérable à deux types d'exécution de code à distance. La première (CVE-2016-0148), de niveau important, peut être causée par une validation incorrecte d'une entrée avant le chargement des bibliothèques. La deuxième, critique, fait référence à la vulnérabilité sur le composant Windows Graphics (CVE-2016-0145). A noter que cette dernière est également présente dans Skype Entreprise 2016, Lync 2010, Lync 2013 et Console Microsoft Live Meeting 2007.

Pour finir, la vulnérabilité CVE-2016-0128 touche les protocoles distants Gestionnaire de compte de sécurité (SAM) et Autorité de sécurité locale (stratégie de domaine) (LSAD). Plus connue sous le nom de Badlock, elle est considérée par Microsoft comme importante. Afin d'être exploitée, la faille nécessite que l'attaquant soit déjà présent sur le réseau de l'entreprise. En effet, les protocoles [MS-SAMR] et [MS-LSAD] sont vulnérables à l'attaque de l'intercepteur actif (aussi connue sous MiTM, voire du singe intercepteur). L'attaquant, en s'insérant dans la connexion entre le client et le serveur, pourra forcer le passage à une version antérieure de Windows RPC ([MS-RPCE]), et ainsi obtenir un accès à la base de données SAM pour obtenir les condensés des mots de passe des administrateurs et élever ses privilèges.

Recommandations

Le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

Documentation

- Avis CERTFR-2016-AVI-120
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-120
- Avis CERTFR-2016-AVI-121
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-121
- Avis CERTFR-2016-AVI-122
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-122
- Avis CERTFR-2016-AVI-123
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-123
- Avis CERTFR-2016-AVI-124
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-124
- Avis CERTFR-2016-AVI-125
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-125
- Badlock
  http://badlock.org/
- Samba
  https://www.samba.org/samba/security/CVE-2016-2118.html
- LSAD
  https://msdn.microsoft.com/fr-fr/library/cc239712.aspx

MS-LSAD https://msdn.microsoft.com/en-us/library/cc234225.aspx
MS-SAM https://msdn.microsoft.com/fr-fr/library/cc245476.aspx
MS-RPCE https://msdn.microsoft.com/fr-fr/library/cc243560.aspx

4 - Rappel des avis émis

Dans la période du 11 au 17 avril 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-117 : Vulnérabilité dans Juniper ScreenOS
- CERTFR-2016-AVI-118 : Vulnérabilité dans F5 BIG-IP
- CERTFR-2016-AVI-119 : Vulnérabilité dans F5 BIG-IP et BIG-IQ
- CERTFR-2016-AVI-120 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-121 : Multiples vulnérabilités dans Microsoft Edge

- CERTFR-2016-AVI-122 : Multiples vulnérabilités dans le composant Microsoft Graphics
- CERTFR-2016-AVI-123 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2016-AVI-124 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-125 : Multiples vulnérabilités dans Microsoft .NET
- CERTFR-2016-AVI-126 : Multiples vulnérabilités dans les produits Adobe
- CERTFR-2016-AVI-127 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-128 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2016-AVI-129 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-130 : Vulnérabilité dans les produits VMware
- CERTFR-2016-AVI-131 : Multiples vulnérabilités dans le noyau Linux de Suse

Gestion détaillée du document

18 avril 2016 version initiale.