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 05 janvier 2015
N° CERTFR-2015-ACT-001

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-001

1 - Vœux du CERT-FR

En ce début d'année, le CERT-FR présente ses meilleurs vœux à l'ensemble de ses lecteurs et de ses partenaires nationaux et internationaux, des secteurs public et privé.

L'année 2014 aura vu le passage du CERTA au CERT-FR. Ce changement d'acronyme marque une réelle évolution en phase avec celle de l'ANSSI en général et du Centre opérationnel SSI en particulier, dont le CERT-FR constitue le point de contact privilégié dans le monde des CERT nationaux et internationaux.

En développant ses compétences métier et en adoptant une structure matricielle pluridisciplinaire, le CERT-FR se veut aujourd'hui être en mesure de mobiliser l'ensemble des compétences et expertises que l'ANSSI peut mettre en œuvre dans les domaines de l'audit, de la veille en vulnérabilités et codes malveillants, de l'analyse de la menace, de la détection d'incident ainsi que de l'alerte et du traitement des cybermenaces qui peuvent affecter les intérêts vitaux de la Nation. Le CERT-FR poursuivra ses efforts en 2015 afin d'améliorer encore ses capacités de prise en compte et de traitement 24 heures sur 24 et 7 jours sur 7.

2014 aura également vu publiée une profusion sans précédent de rapports et de « révélations » qui ont permis au plus grand nombre de percevoir l'étendue de la cybermenace qui pèse tant sur les entreprises que sur les organisations gouvernementales. Il revient à chaque acteur de la cybersécurité et de la cyberdéfense d'intégrer ces menaces protéiformes pour mettre en œuvre les moyens permettant d'y faire face. Dans ce domaine, le pragmatisme doit demeurer de rigueur. En effet, le CERT-FR est encore trop souvent amené à traiter des incidents qui auraient pu facilement être évités par l'application des mesures les plus élémentaires d'hygiène informatique, telles la tenue à jour des systèmes de leurs correctifs de sécurité, la mise en place d'une politique de gestion des mots de passe, la séparation des usages utilisateurs et administrateurs, la supervision minimale des évènements de sécurité, etc.

Cette perception des risques doit également pousser l'ensemble des acteurs de la cybersécurité à densifier leurs coopérations opérationnelles avec les partenaires publics et privés susceptibles de pouvoir les aider à y faire face. En effet, au regard de l'étendue et de la complexité toujours croissantes des menaces qui pèsent sur les systèmes d'information, aucune entité ne peut plus aujourd'hui prétendre pouvoir être en mesure de les affronter seule. Chaque acteur doit donc mettre en place des politiques d'échanges maîtrisés d'informations sur les menaces et les moyens de s'en protéger ou de s'en défendre, mais également pour rechercher à faire interagir en complémentarité les différents champs de compétences nécessaires afin de développer et rentabiliser les ressources et expertises encore trop souvent bien insuffisantes.

Dans ce cadre, l'ANSSI développe la qualification de prestataires de confiance afin de constituer des relais dans le domaine de la cyberdéfense. Après la qualification de prestataires d'audit en sécurité de systèmes d'information en 2014, l'ANSSI va lancer en 2015 une phase expérimentale de qualification de prestataires de réponse aux incidents de sécurité. Un référentiel d'exigences applicables aux prestataires en détection d'incidents sera également publié pour appel à commentaire en janvier 2015.

Le CERT-FR vous souhaite une bonne année 2015.

2 - Actualité des mécanismes de protections contre les corruptions en mémoire noyau

Présentation

Le noyau («*kernel*» en anglais) est le composant fondamental des systèmes d'exploitation généralistes modernes. Il assure l'interface entre les applications classiques s'exécutant en espace utilisateur et le matériel (mémoire vive, stockage de masse, interfaces réseau, etc.). Il est le garant de la sécurité du système et sa compromission est synonyme de maîtrise totale de l'attaquant sur l'ensemble des ressources de la machine. Afin de limiter les possibilités d'exploitation de failles de sécurité au niveau du noyau, plusieurs mécanismes de protection font régulièrement l'objet de développements.

Cet article se propose de présenter des méthodes récemment publiées de contournement de tels mécanismes sous Linux et les contre-mesures associées.

Description de la vulnérabilité

Considérons un bogue de type « corruption mémoire » affectant le noyau Linux, et permettant à un attaquant de modifier une partie de la mémoire manipulée par celui-ci. L'exploitation d'une telle faille consiste en général à remplacer le contenu d'un emplacement particulier, dans l'espace mémoire noyau, par une adresse pointant vers une zone contrôlée par l'attaquant, en espace utilisateur. Au lieu d'exécuter une routine légitime en espace noyau, l'attaquant force ainsi le système à exécuter du code qu'il aura préalablement placé en espace utilisateur. Ce code sera exécuté avec les privilèges du noyau. L'attaquant peut également modifier des références à des données, et les faire pointer vers des zones de l'espace utilisateur. Dans les deux cas (code ou données), le noyau est amené à manipuler une zone mémoire située en espace utilisateur et contrôlée par l'attaquant .

Des mécanismes ont été implémentés pour contrecarrer ces attaques. En particulier, le patch *Grsecurity* fournit deux fonctionnalités empêchant le noyau de manipuler directement de la mémoire allouée pour l'espace utilisateur : `UDEREF` (pour la manipulation de données) et `KERNEXEC` (pour l'exécution de code). Les processeurs modernes offrent également des fonctionnalités matérielles similaires (par exemple `SMEP` et `SMAP` pour les processeurs Intel). Un accès direct à la mémoire utilisateur depuis l'espace noyau est théoriquement impossible sur des systèmes durcis utilisant ces fonctionnalités.

Des chercheurs de l'université de Colombia se sont intéressés à des méthodes de contournement de ces mécanismes. Ils ont présenté un article intitulé « *ret2dir: Rethinking Kernel Isolation* » lors de la conférence USENIX, en août 2014. Leur attaque repose sur l'exploitation d'une optimisation couramment utilisée par les allocateurs de mémoire en espace noyau. Afin d'éviter de coûteuses modifications de la table des pages du noyau à chaque allocation dynamique, une grande partie de la mémoire physique est projetée directement dans l'espace du noyau, y compris celle allouée pour l'espace utilisateur (cette projection est dénommée « `physmap` »). Une conséquence directe est que chaque emplacement de mémoire physique alloué pour l'espace utilisateur dispose également d'une adresse virtuelle en espace noyau.

Les auteurs parlent de « synonymes » pour désigner deux adresses virtuelles (une en espace utilisateur, une en espace noyau) pointant vers une même zone mémoire physique.

Prenons un exemple : un utilisateur alloue de la mémoire, et le système lui attribue l'adresse `0xBEEF000`, pour un numéro de page 1904 (information disponible dans le pseudo-système de fichier /proc). Pour l'architecture x86, la physmap est située à l'adresse fixe `0xC0000000`, et les pages ont pour taille 4096 octets. Le synonyme de l'adresse utilisateur `0xBEEF0000` en espace noyau sera donc :
`0xC0000000 + 4096*1904 = 0xC0770000`.

Le contournement de `UDEREF` et `KERNEXEC` est alors théoriquement possible d'après l'article. Il suffit à l'attaquant d'allouer une zone en espace utilisateur pour y stocker le code malveillant ou bien les données modifiées, de calculer l'adresse synonyme correspondante en espace noyau, et de déclencher la vulnérabilité. Le nom de la méthode « *ret2dir* » fait allusion à la manipulation par le noyau d'une projection mémoire directe (en anglais : "return to direct-mapped memory"). Dans ces conditions, le noyau ne manipulera que du code ou des données projetés en espace noyau, mais contrôlés depuis l'espace utilisateur. Les contre-mesures précitées seront ainsi inopérantes. Les auteurs annoncent avoir contourné les protections `UDEREF` et `KERNEXEC` sur les architectures x86, x86-64, AArch32 et AArch64.

Contre-mesures proposées

L'article propose également une contre-mesure sous la forme d'un patch pour le noyau Linux, mais celui-ci n'est pas intégré au code source « vanille ». Ce type d'attaque avancée illustre un point fondamental dans la sécurité des systèmes d'information : quel que soit le niveau de durcissement d'un système exposé à des attaquants, il existe probablement un moyen de le compromettre.

À titre d'exemple, il faut notamment relativiser la confiance que l'on peut accorder à des architectures de sécurité de type « bastion », dans lesquelles un système unique constitue un maillon critique de la chaîne. Même s'il fait l'objet d'un durcissement particulier, la possibilité qu'il soit compromis un jour ne peut être écartée.

Il convient donc de ne pas accorder à ce type de serveur une confiance aveugle, qui se traduirait au niveau technique par un accès illimité au reste du système d'information. Il est néanmoins possible de complexifier le travail d'un attaquant en appliquant le principe de défense en profondeur : même si aucune mesure de sécurité définitive n'existe, il faut s'efforcer de durcir de nombreux aspects du système, et pas uniquement le noyau. Il est également souhaitable de procéder à une diminution des fonctionnalités supportées par le noyau, afin de limiter la surface d'attaque.

Conclusion

Cette minimisation ne doit pas empêcher la mise à jour rapide du système : il convient donc de s'assurer préalablement de disposer des ressources humaines et techniques nécessaires pour supporter le processus de mise à jour sur le long terme. En effet, la minimisation des fonctionnalités supportées par un noyau demande souvent de procéder à un travail de recompilation. L'ANSSI a publié un ensemble de recommandations permettant de durcir un système Linux.

Documentation

- Présentation USENIX « *ret2dir: Rethinking Kernel Isolation* » :
  https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kemerlis
- Recommandations de sécurité relatives à un système GNU/Linux :
  http://www.ssi.gouv.fr/IMG/pdf/NP_Linux_NoteTech_1_1.pdf

3 - Rappel des avis émis

Dans la période du 29 décembre 2014 au 04 janvier 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-542 : Multiples vulnérabilités dans IBM Security Network Intrusion Prevention System
- CERTFR-2014-AVI-543 : Vulnérabilité dans IBM i
- CERTFR-2014-AVI-544 : Multiples vulnérabilités dans GNU project GnuPG
- CERTFR-2015-AVI-001 : Vulnérabilité dans IBM Sterling Connect:Direct for UNIX
- CERTFR-2015-AVI-002 : Vulnérabilité dans Noyau Linux

Gestion détaillée du document

05 janvier 2015 version initiale.