Présentation de solution

BERserk : la contre-attaque

Ou comment restaurer la confiance de l'utilisateur dans les connexions approuvées

La définition de la confiance est-elle en train de changer ? Les attaques telles que BERserk et Heartbleed ébranlent la confiance que placent les utilisateurs dans des protocoles comme SSL (Secure Sockets Layer) et TLS (Transport Layer Security). Cette confiance s'évanouit dès lors que la confidentialité, l'intégrité et l'authenticité des informations sont mises en doute. Comment s'assurer que votre entreprise est protégée contre l'abus de confiance commis par BERserk ?

Qu'est-ce que BERserk ?

Cette vulnérabilité est abordée en détail dans le **Rapport de McAfee sur le paysage des menaces de novembre 2014**. BERserk est une vulnérabilité de type falsification des signatures, rendue possible par la manière dont RSA vérifie ces signatures. Mozilla a corrigé la bibliothèque cryptographique vulnérable Mozilla NSS (Network Security Services), communément utilisée dans le navigateur web Firefox, mais celle-ci se trouve également dans Thunderbird, SeaMonkey, Google Chrome et d'autres produits. BERserk permet à des pirates d'exécuter des attaques de type « intercepteur » (*man-in-the-middle*), dans le cadre desquelles ils falsifient les signatures RSA et contournent ainsi le mécanisme d'authentification des sites web utilisant les protocoles SSL/TLS.

BERserk est une variante de Bleichenbacher PKCS#1 version 1.5, une vulnérabilité de falsification des signatures RSA décrite dans l'entrée **CVE-2006-4339**. La faille réside dans l'analyse syntaxique incorrecte de l'encodage ASN.1 pendant la vérification des signatures, l'attaque exploitant le fait qu'un champ respectant les règles BER (*Basic Encoding Rules*) peut être défini de manière à accepter de nombreux octets de données. Dans les implémentations vulnérables, l'analyse syntaxique passe outre ces octets dans certains champs.

Un pirate peut ainsi falsifier des certificats RSA sans connaître la clé privée RSA correspondante. Il a été établi que des certificats RSA 1 024 bits et 2 048 bits ont été falsifiés de la sorte, la fausse chaîne de certificat étant acceptée comme fiable par Mozilla NSS.

intel Security

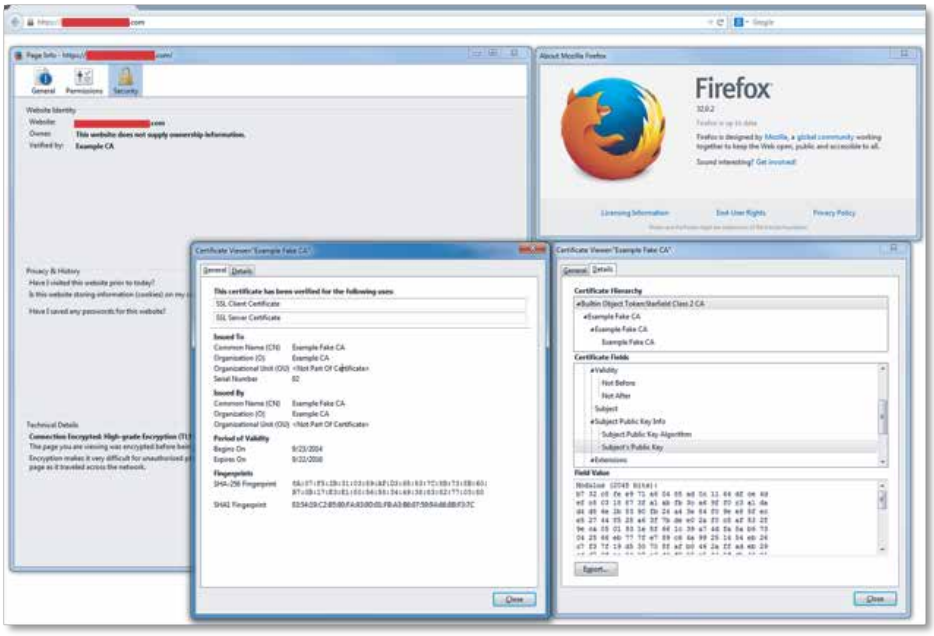

Figure 1. Certificat falsifié vu dans Firefox

Comment sommes-nous affectés par BERserk ? BERserk et les vulnérabilités similaires mettent à mal non seulement la sécurité des sessions faisant appel à des connexions SSL/TLS, mais aussi la confiance que nous leur accordons. Un cybercriminel peut établir une multitude de sessions MITM à l'aide de certificats RSA falsifiés, ce qui lui permet de pirater des sessions, de manipuler les entrées et les sorties ou encore de voler des données sensibles.

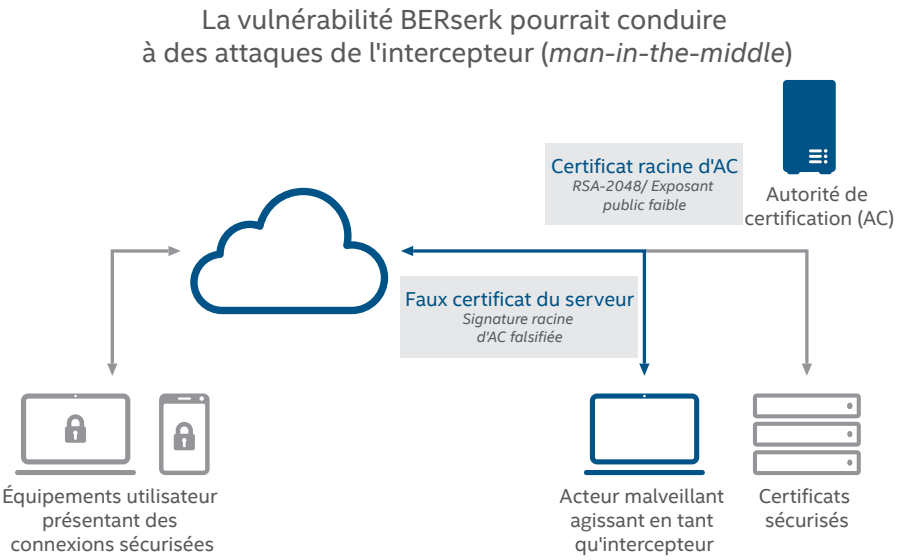

Figure 2. BERserk permet aux pirates de falsifier des signatures RSA et donc de contourner le mécanisme d'authentification de nombreux sites web.

Que faire dans l'immédiat ?
Assurez-vous que vous employez les derniers correctifs publiés par Mozilla pour la bibliothèque cryptographique Mozilla NSS, Firefox, Thunderbird, SeaMonkey et d'autres produits Mozilla. Google a également publié des correctifs pour son navigateur Google Chrome et son système d'exploitation Google Chrome OS, dans la mesure où ces produits utilisent eux aussi la bibliothèque cryptographique vulnérable.

Comment McAfee vous aide-t-il à vous protéger contre BERserk ?

Les produits McAfee sont en mesure de vous protéger contre les attaques qui tentent d'exploiter la vulnérabilité BERserk. Ainsi, McAfee Vulnerability Manager peut analyser vos systèmes pour identifier et signaler ceux qui sont vulnérables à BERserk. McAfee Application Control peut quant à lui faire en sorte que les applications vulnérables ne soient pas autorisées à s'exécuter dans votre environnement avant d'avoir fait l'objet des corrections adéquates.

McAfee Vulnerability Manager
Les attaques telles que BERserk sont une illustration parfaite du paysage des menaces en perpétuelle évolution auxquelles les entreprises sont confrontées de nos jours. Cela dit, déterminer si vous courez effectivement un risque et évaluer votre degré de vulnérabilité à ces nouvelles attaques peuvent apparaître comme des épreuves insurmontables. Voici, à titre d'exemple, comment **McAfee Vulnerability Manager** et **McAfee Asset Manager** peuvent aider votre entreprise à comprendre les vulnérabilités telles que BERserk et à prendre les mesures nécessaires pour combler efficacement les failles éventuelles :

- **Analyse complète des vulnérabilités —** McAfee Vulnerability Manager est un produit autonome hautement évolutif pour la découverte des hôtes, la gestion des actifs, l'évaluation des vulnérabilités et la génération de rapports sur tous les équipements réseau. Il peut identifier le risque de succomber à BERserk en recherchant les systèmes qui exécutent des versions vulnérables de Firefox, de Chrome et d'autres produits qui emploient la bibliothèque cryptographique Mozilla NSS.
- **Personnalisation des analyses en fonction des nouvelles menaces —** L'outil FSL (Foundstone Scripting Language) Editor peut optimiser les contrôles prédéfinis et les mises à jour pour améliorer la détection des menaces et des vulnérabilités « jour zéro » telles que BERserk, grâce à la création de scripts et de contrôles personnalisés destinés à évaluer votre environnement. McAfee Vulnerability Manager peut désormais détecter les systèmes vulnérables à BERserk au moyen de ses contrôles prédéfinis, et ce depuis le 24 septembre 2014.
- **Rapports et corrections flexibles —** McAfee Vulnerability Manager et McAfee Asset Manager fonctionnent de concert pour assurer une gestion et une surveillance automatisées de l'analyse, de la correction, de la mise en œuvre et de la génération de rapports. Vous évitez ainsi les exercices d'alerte et les processus ponctuels fastidieux, vous éliminez les erreurs et vous protégez plus de systèmes avec efficacité.
- **Connaissance de votre niveau de risque —** McAfee Asset Manager indique à l'entreprise les systèmes vulnérables à BERserk en mettant en corrélation des analyses de vulnérabilités avec des analyses de découverte des hôtes. L'identification en temps réel des systèmes précis qui exécutent des versions vulnérables de Firefox et d'autres applications permet de perdre moins de temps en spéculations et d'en consacrer davantage aux mesures correctives.

McAfee Application Control
Protéger votre entreprise contre le code et les applications indésirables, tels que ceux vulnérables à BERserk, est crucial. **McAfee Application Control** permet à votre entreprise de contrôler les applications autorisées à s'exécuter dans votre environnement par le truchement de listes blanches dynamiques et de stratégies de mise en œuvre, qui s'appliquent tant aux terminaux connectés qu'à ceux hors connexion.

- **Listes blanches dynamiques —** Cette fonction permet à l'entreprise de gérer efficacement les applications sur liste blanche en développant automatiquement cette dernière à mesure que les systèmes sont corrigés et mis à jour. McAfee Application Control peut réduire votre exposition à BERserk en bloquant l'exécution d'applications appelant le code de vérification de signatures RSA vulnérable.
- **Réputation des fichiers —** L'intégration à **McAfee Global Threat Intelligence** permet à McAfee Application Control d'interroger les flux d'informations en temps réel définissant les types de fichiers dont la réputation est bonne, mauvaise ou inconnue, de façon à aider l'entreprise à identifier les nouvelles vulnérabilités telles que BERserk.
- **Protection des équipements, qu'ils soient connectés ou hors connexion —** Les contrôles sont mis en œuvre sur les serveurs, les machines virtuelles, les terminaux et les équipements fixes tels que les terminaux de point de vente, qu'ils soient connectés ou non.

BERserk est une vulnérabilité grave qui peut exposer vos systèmes à un large éventail d'attaques. La technologie de sécurité McAfee peut identifier les systèmes vulnérables et bloquer les attaques qui exploitent BERserk.

Pour plus d'informations sur BERserk, consultez les sources suivantes :

- **BERserk vulnerability: Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Vulnérabilité BERserk : Partie 1 — Attaque de type falsification des signatures RSA due à l'analyse incorrecte de l'élément DigestInfo codé ASN.1 dans PKCS#1 version 1.5)
- **BERserk vulnerability: Part 2: Certificate forgery in Mozilla NSS** (Vulnérabilité BERserk : Partie 2 — Falsification de certificats dans Mozilla NSS)
- Computer Emergency Response Team : **VU#772676**
- National Vulnerability Database : **CVE-2014-1568**
- Blog McAfee : **http://blogs.mcafee.com/executive-perspectives/need-know-berserk-mozilla**

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com