Resumen de la solución

Contraataque dirigido a BERserk

Restablecemos la "confianza" en la conectividad fiable.

¿Está cambiando lo que entendemos por "de confianza"? Ataques como BERserk y Heartbleed ponen en jaque la confianza que se ha puesto en los protocolos Secure Sockets Layer (SSL) y Transport Layer Security (TLS). Dicha confianza se desvanece cuando la privacidad, la integridad y la autenticidad de nuestra información se ve cuestionada. ¿Cómo puede asegurarse de que su empresa esté protegida frente a los abusos de confianza de BERserk?

¿Qué es BERserk?

En el **informe de McAfee sobre amenazas de noviembre de 2014** se analiza en profundidad la vulnerabilidad BERserk. BERserk es una vulnerabilidad basada en la falsificación de firmas que existe debido al método que el sistema RSA utiliza para verificar las firmas. Mozilla ha revisado la biblioteca criptográfica vulnerable Mozilla Network Security Services (NSS), que se suele utilizar en el navegador web Firefox, pero también está presente en Thunderbird, SeaMonkey, Google Chrome y otros productos. BERserk permite a usuarios maliciosos perpetrar ataques de intermediario permitiéndoles falsificar firmas RSA y burlar la autenticación en los sitios web que emplean los protocolos SSL/TLS.

BERserk es una variación de la vulnerabilidad de falsificación de firmas RSA PKCS#1 v1.5 de Bleichenbacher definida en **CVE-2006-4339**. El fallo está en el análisis incorrecto de la codificación ASN.1 durante la verificación de las firmas, y el ataque aprovecha el hecho de que la longitud de un campo, según las reglas de codificación básicas (BER), se pueda establecer para utilizar una gran cantidad de bytes de datos. En las implementaciones que son vulnerables, esta presencia de cantidades de datos tan elevadas hace que dicha información se ignore en el análisis.

Esto significa que un delincuente puede falsificar certificados RSA sin conocer la clave privada RSA correspondiente. Tantos los certificados RSA de 1024 bits como los de 2048 bits se han conseguido falsificar y Mozilla NSS ha confiado en esta cadena de certificados falsificados.

intel Security

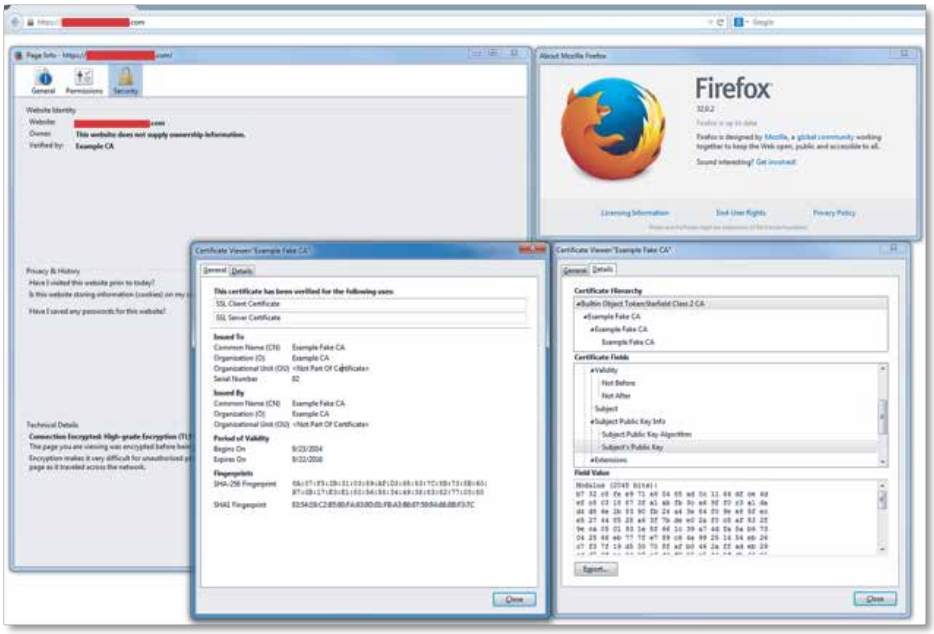

Figura 1. Certificado falsificado como aparece en Firefox.

¿Cómo nos afecta BERserk? BERserk y otras vulnerabilidades similares menoscaban la confianza y la seguridad inherentes en las sesiones de comunicación basadas en SSL/TLS. Un agresor puede establecer una sesión de ataque de intermediario en muy distintos casos mediante certificados RSA falsificados, lo que le permitiría apropiarse de sesiones, manipular datos de entrada y de salida, y robar información confidencial.

Figura 2. BERserk permite a los agresores falsificar firmas RSA y burlar la autenticación en gran cantidad de sitios web.

¿Qué se puede hacer de manera inmediata?
Asegúrese de estar utilizando los parches más recientes de la biblioteca criptográfica Mozilla NSS, Firefox, Thunderbird, SeaMonkey y otros productos de Mozilla. Google también ha publicado parches para Google Chrome y Chrome OS, dado que estos productos también utilizan la biblioteca vulnerable.

¿Cómo puede ayudar McAfee a mejorar la protección frente a BERserk?

Los productos de McAfee le ofrecen protección frente a ataques diseñados para aprovechar la vulnerabilidad BERserk. McAfee Vulnerability Manager examina ampliamente sus sistemas para identificar e informar de aquellos que son vulnerables a BERserk. Con McAfee Application Control, tendrá la garantía de que las aplicaciones vulnerables a BERserk no se ejecuten en su entorno hasta que se hayan corregido.

McAfee Vulnerability Manager
Ataques como BERserk son ejemplos de las amenazas en constante cambio que afectan a las empresas de hoy en día. Ser consciente de a qué riesgos está expuesto y de hasta qué punto es vulnerable a estos nuevos ataques puede resultar una tarea abrumadora. A continuación, detallamos algunas de las formas en las que **McAfee Vulnerability Manager**, junto con **McAfee Asset Manager**, puede contribuir a que su empresa esté al tanto de vulnerabilidades como BERserk y tome las medidas necesarias para ponerles remedio de manera eficaz:

- **Análisis completo de vulnerabilidades:** McAfee Vulnerability Manager es un producto independiente y altamente escalable de descubrimiento de hosts, administración de activos, evaluación de vulnerabilidades y generación de informes en cualquier dispositivo conectado a la red. McAfee Vulnerability Manager comprueba la presencia de BERserk buscando sistemas que ejecuten versiones vulnerables de Firefox, Chrome y otros productos que utilicen la biblioteca criptográfica vulnerable Mozilla NSS.
- **Análisis personalizados de nuevas amenazas:** el editor Foundstone Scripting Language (FSL) es capaz de ampliar las comprobaciones predefinidas y las actualizaciones para mejorar la detección de amenazas y vulnerabilidades zero-day, como BERserk, escribiendo secuencias de comandos personalizadas y comprobaciones para evaluar su entorno. McAfee Vulnerability Manager ahora es capaz de detectar sistemas vulnerables a BERserk en el marco de sus comprobaciones predefinidas a partir del 24 de septiembre de 2014.
- **Generación de informes y medidas correctivas de gran flexibilidad:** McAfee Vulnerability Manager y McAfee Asset Manager funcionan en colaboración para proporcionar una supervisión y una administración automatizadas de los análisis, las medidas correctivas, la implementación y la generación de informes. De esta manera, podrá evitar laboriosos simulacros de emergencia y procesos ad hoc, eliminar errores y proteger un mayor número de sistemas de forma más eficaz.
- **Conozca su nivel de exposición:** McAfee Asset Manager permite a su empresa saber qué sistemas son vulnerables a BERserk mediante la correlación de análisis de vulnerabilidades con análisis de descubrimiento de hosts. La identificación en tiempo real de los sistemas que están ejecutando versiones vulnerables de Firefox y otras aplicaciones permite reducir el tiempo para saber si se corren riesgos, y disponer de más tiempo para aplicar medidas correctivas.

McAfee Application Control

Proteger su empresa de aplicaciones y código no deseados, como los que son vulnerables a BERserk, es fundamental. **McAfee Application Control** permite a su empresa controlar qué aplicaciones se pueden ejecutar en su entorno por medio de listas blancas dinámicas y directivas de implementación, tanto en los endpoints conectados como en los desconectados.

- **Listas blancas dinámicas:** permita que su organización administre de forma eficaz sus aplicaciones desarrollando de forma automática una lista blanca a medida que los sistemas se revisen con parches y se actualicen. McAfee Application Control reduce su exposición a BERserk impidiendo que se ejecuten las aplicaciones que invocan código de verificación de firmas RSA vulnerable.
- **Reputación de archivos:** la integración con **McAfee Global Threat Intelligence** permite a McAfee Application Control consultar información en tiempo real sobre tipos de archivos conocidos, legítimos y maliciosos, y desconocidos para asegurarse de que su empresa esté informada de vulnerabilidades como BERserk.
- **Protección con conexión o sin ella:** implemente controles en los servidores conectados y desconectados, las máquinas virtuales, los endpoints y los dispositivos fijos, como los terminales punto de venta.

BERserk es una vulnerabilidad grave que puede exponer sus sistemas a una amplia diversidad de ataques. La tecnología de seguridad de McAfee puede identificar sistemas vulnerables y frustrar ataques que aprovechan BERserk.

Para obtener más información sobre BERserk:

- **BERserk vulnerability: Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Vulnerabilidad BERserk: Parte 1: Ataque de falsificación de firmas RSA debido al análisis incorrecto de la codificación ASN.1 DigestInfo en PKCS#1 v1.5)
- **BERserk vulnerability: Part 2: Certificate forgery in Mozilla NSS** (Vulnerabilidad BERserk: Parte 2: Falsificación de certificados en Mozilla NSS)
- Computer Emergency Response Team: **VU#772676**
- National Vulnerability Database: **CVE-2014-1568**
- Blog de McAfee: **http://blogs.mcafee.com/executive-perspectives/need-know-berserk-mozilla**

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com