Kurzvorstellung

# Gegenangriff auf BERserk

**Wiederherstellen des Vertrauens in vertrauenswürdige Verbindungen**

Ändert sich gerade die Definition dessen, was wir als Vertrauenswürdigkeit bezeichnen? Angriffe wie BERserk und Heartbleed erschüttern das Vertrauen in die Sicherheitsverfahren SSL (Secure Sockets Layer) und TLS (Transport Layer Security). Vertrauenswürdigkeit ist nicht mehr gegeben, wenn Zweifel an der die Vertraulichkeit, Integrität und Authentizität unserer Daten entstehen. Wie können Sie sicherstellen, dass Ihr Unternehmen davor geschützt ist, dass BERserk die Vertrauenswürdigkeit untergräbt?

## Was ist BERserk?

BERserk wird ausführlich im **McAfee Labs Threat-Report für November 2014** vorgestellt. Beim BERserk-Angriff wird eine Schwachstelle bei der Signaturüberprüfung von RSA ausgenutzt, um auf diese Weise Signaturen zu fälschen. Mozilla veröffentlichte einen Patch der betroffenen Kryptobibliothek Mozilla Network Security Services (NSS), die beispielsweise beim Web-Browser Firefox genutzt wird. Mozilla NSS kommt jedoch auch bei Thunderbird, SeaMonkey, Google Chrome und weiteren Produkten zum Einsatz. Mit BERserk können Angreifer Man-in-the-Middle-Attacken durchführen, indem sie RSA-Signaturen fälschen und auf diese Weise die Authentifizierung von Webseiten mit SSL/TLS aushebeln.

BERserk ist eine Variante der Schwachstelle Bleichenbacher PKCS#1 v1.5 RSA Signature Forgery (RSA-Signaturfälschung), die in **CVE-2006-4339** definiert ist. Das Problem liegt in der fehlerhaften Verarbeitung der ASN.1-Kodierung während der Signaturüberprüfung. Der Angriff nutzt die Tatsache aus, dass die Länge eines Feldes in den grundlegenden Kodierungsfehlern (Basic Encoding Rules, BER) so verändert werden kann, dass viele Byte an Daten genutzt werden. In anfälligen Implementierungen führt das Vorhandensein vieler Bytes dazu, dass sie bei der Verarbeitung übersprungen werden.

Ein Angreifer kann also RSA-Zertifikate fälschen, ohne den dazugehörigen privaten RSA-Schlüssel zu kennen. Bisher wurden bereits RSA-Zertifikate mit 1024 Bit sowie mit 2048 Bit nachweislich gefälscht, und Mozilla NSS vertraute der gefälschten Zertifikatkette.

intel Security

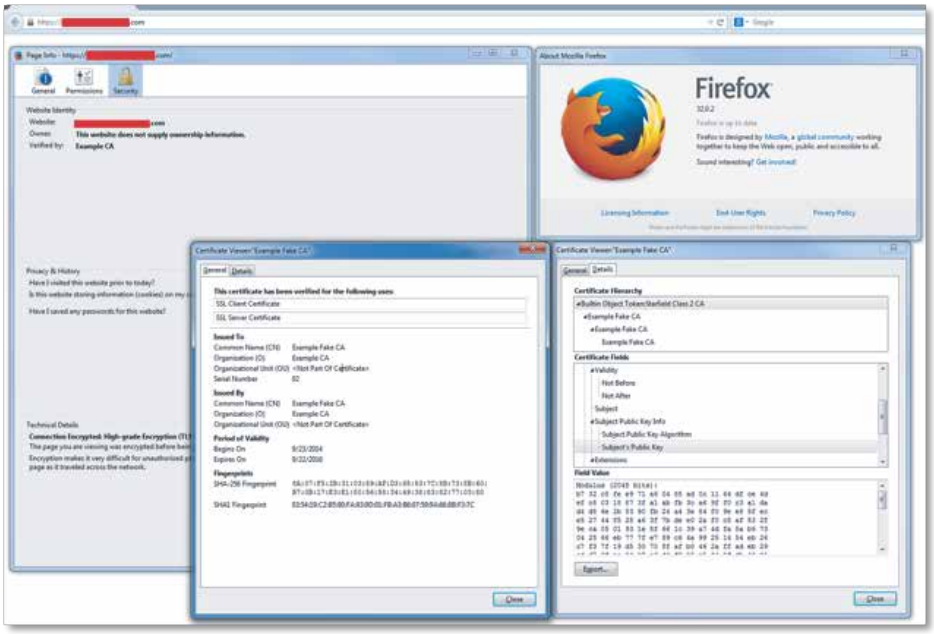


**Abbildung 1.** Gefälschtes Zertifikat in Firefox

Inwiefern sind wir von BERserk betroffen? BERserk und ähnliche Schwachstellen untergraben die Vertrauenswürdigkeit und Sicherheit von SSL/TLS-Sitzungen. Ein Angreifer kann mit gefälschten RSA-Zertifikaten in beliebigen Szenarien eine Man-in-the-Middle-Sitzung etablieren. Dadurch erhält er die Möglichkeit, Sitzungen zu kapern, Ein- und Ausgaben zu manipulieren oder sensible Daten zu erfassen.

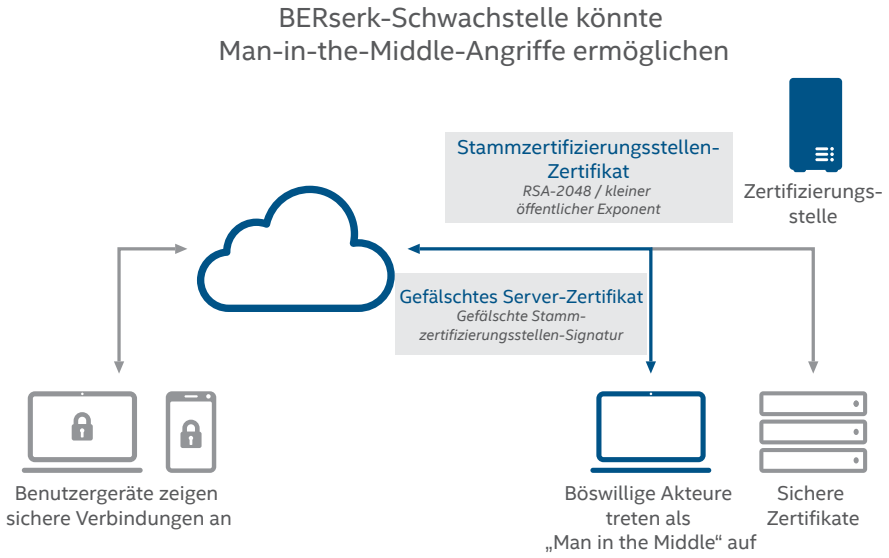


**Abbildung 2.** Mit BERserk können Angreifer RSA-Signaturen fälschen und die Authentifizierung vieler Webseiten unterlaufen

**Was kann kurzfristig getan werden?**
Überprüfen Sie, ob Sie die neuesten Patches von Mozilla für die Mozilla NSS-Kryptobibliothek, Firefox, Thunderbird, SeaMonkey und andere Mozilla-Produkte installiert haben. Google hat ebenfalls Patches für Google Chrome und Chrome OS veröffentlicht, da diese Produkte ebenfalls die anfällige Bibliothek nutzen.

## Wie kann McAfee vor BERserk schützen?

McAfee-Produkte können Sie vor Angriffen schützen, die die BERserk-Schwachstelle ausnutzen. McAfee Vulnerability Manager kann Ihre Systeme umfassend untersuchen, um alle zu identifizieren und zu melden, die für BERserk anfällig sind. McAfee Application Control kann gewährleisten, dass Anwendungen, die für BERserk anfällig sind, erst dann in Ihrer Umgebung ausgeführt werden dürfen, wenn ihre Schwachstellen behoben wurden.

**McAfee Vulnerability Manager**
Angriffe wie BERserk sind ein Sinnbild für den ständigen Wandel der aktuellen Bedrohungssituation für Unternehmen. Es kann zweitaufwändig und komplex sein zu erkennen, ob Sie für diese neuen Angriffe anfällig sind. Im Folgenden stellen wir einige Möglichkeiten vor, wie **McAfee Vulnerability Manager** zusammen mit **McAfee Asset Manager** Ihrem Unternehmen dabei helfen kann, Schwachstellen wie BERserk zu verstehen und die notwendigen Maßnahmen zu ihrer Beseitigung zu ergreifen:

- **Umfassende Schwachstellen-Scans:** McAfee Vulnerability Manager ist ein stark skalierbares eigenständiges Produkt für Host-Erkennung, Ressourcen-Management, Schwachstellenanalyse sowie Berichterstellung zu allen Geräten, die mit dem Netzwerk verbunden sind. McAfee Vulnerability Manager kann nach BERserk suchen, indem überprüft wird, ob auf den Systemen anfällige Versionen von Firefox, Chrome und anderen Produkten mit der anfälligen Mozilla NSS-Kryptobibliothek verwendet werden.
- **Anpassung von Scans an neue Bedrohungen:** Der FSL-Editor (Foundstone Scripting Language) kann vordefinierte Überprüfungen und Aktualisierungen für Zero-Day-Bedrohungen und Schwachstellen wie BERserk verbessern, indem die Erstellung benutzerdefinierter Skripte und Überprüfungen zur Analyse Ihrer Umgebung ermöglicht wird. McAfee Vulnerability Manager kann seit dem 24. September 2014 mithilfe der vordefinierten Überprüfungen Systeme erkennen, die für BERserk anfällig sind.
- **Flexible Berichterstellung und Problembehebung:** McAfee Vulnerability Manager und McAfee Asset Manager arbeiten zusammen, um die automatisierte Überwachung und Verwaltung für Scans, Problembehebung, Durchsetzung und Berichterstellung bereitzustellen. Dadurch können Sie zeitaufwändige Alarmübungen, Ad-hoc-Prozesse sowie Fehler vermeiden und mehr Systeme effektiv schützen.
- **Kennen Sie Ihre Gefährdung:** McAfee Asset Manager zeigt Ihrem Unternehmen, welche Systeme für BERserk anfällig sind, indem Schwachstellen-Scans mit Scans zur Host-Erkennung korreliert werden. Durch die Echtzeiterkennung von Systemen, die anfällige Versionen von Firefox und anderen Anwendungen ausführen, haben Sie erheblich schneller Sicherheit darüber, ob Sie gefährdet sind, und können schneller mit der Problembehebung beginnen.

**McAfee Application Control**

Der Schutz Ihres Unternehmens vor unerwünschtem Code und Anwendungen, darunter auch für BERserk anfälligen, ist unabdingbar. Mit **McAfee Application Control** kann Ihr Unternehmen kontrollieren, welche Anwendungen in Ihrer Umgebung ausgeführt werden. Dabei kommen dynamische Whitelists und Durchsetzungsrichtlinien für vernetzte und eigenständige Endgeräte zum Einsatz.

- **Dynamische Whitelists:** Damit kann Ihr Unternehmen Anwendungen, die auf einer Whitelist geführt werden, effektiv verwalten, indem die Whitelist automatisch erweitert wird, sobald die Systeme gepatcht und aktualisiert werden. McAfee Application Control kann Ihre Anfälligkeit für BERserk verringern, indem die Ausführung von Anwendungen verhindert wird, die den anfälligen RSA-Signaturprüfungs-Code aufrufen.
- **Datei-Reputation:** Durch die Integration von **McAfee Global Threat Intelligence** kann McAfee Application Control Echtzeitinformationen zu gefährlichen, ungefährlichen und unbekannten Dateitypen abrufen, sodass Ihr Unternehmen über neue Schwachstellen wie BERserk informiert bleibt.
- **Schutz mit und ohne Vernetzung:** Setzen Sie Kontrollen auf verbundenen oder getrennten Servern, virtuellen Maschinen, Endgeräten und Geräten mit fester Funktion wie Kassenterminals durch.

BERserk ist eine schwerwiegende Schwachstelle, mit der eine große Bandbreite an Angriffen auf Ihre Systeme durchgeführt werden kann. Die McAfee-Sicherheitstechnologien können anfällige Systeme erkennen und Angriffe blockieren, die BERserk ausnutzen.

Weitere Informationen zu BERserk:

- **BERserk vulnerability: Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Bericht zur BERserk-Schwachstelle: Teil 1: Angriff mit RSA-Signaturfälschung aufgrund falscher Verarbeitung von mit ASN.1 kodierter DigestInfo in PKCS#1 v1.5)
- **BERserk vulnerability: Part 2: Certificate forgery in Mozilla NSS** (Bericht zur BERserk-Schwachstelle: Teil 2: Zertifikatfälschung in Mozilla NSS)
- Computer Emergency Response Team: **VU#772676**
- National Vulnerability Database: **CVE-2014-1568**
- McAfee-Blog: **http://blogs.mcafee.com/executive-perspectives/need-know-berserk-mozilla**

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee und das McAfee-Logo sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2014 McAfee, Inc. 61516brf_counter-berserk_1214

**McAfee. Part of Intel Security.**
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com