Resumo de solução

Contra-ataque à BERserk

Restauração da "confiança" na conectividade confiável

A definição de confiança está mudando? Ataques como BERserk e Heartbleed abalam a boa-fé depositada até então em protocolos Secure Sockets Layer (SSL) e Transport Layer Security (TLS). Perde-se a confiança quando a privacidade, a integridade e a autenticidade das nossas informações são questionadas. Como você pode garantir que sua empresa está protegida contra o abuso de confiança da BERserk?

O que é a BERserk?

A BERserk é discutida em detalhes no **Relatório do McAfee Labs sobre ameaças: novembro de 2014**. Trata-se de uma vulnerabilidade de falsificação de assinatura que existe graças à forma como a RSA verifica assinaturas. A Mozilla corrigiu a vulnerável biblioteca de criptografia Mozilla Network Security Services (NSS), que é frequentemente usada no navegador da Web Firefox, mas que também pode ser encontrada no Thunderbird, SeaMonkey, Google Chrome e em outros produtos. A BERserk permite que pessoas maliciosas realizem ataques de interceptação, possibilitando que falsifiquem assinaturas RSA e ignorem a autenticação a sites que usam SSL/TLS.

A BERserk é uma variação da vulnerabilidade de falsificação de assinatura RSA Bleichenbacher PKCS#1 v1.5 definida em **CVE-2006-4339**. A falha está na análise incorreta da codificação ASN.1 durante a verificação de assinatura, e o ataque explora o fato de que o comprimento de um campo segundo as regras básicas de codificação (BER) pode ser definido para utilizar diversos bytes de dados. Em implementações que estão vulneráveis, a presença de muitos bytes faz com que eles sejam ignorados durante a análise.

Isso significa que um atacante pode forjar certificados RSA sem nenhum conhecimento da chave privada RSA correspondente. Já foi comprovado que ambos os certificados RSA de 1.024 bits e de 2.048 bits foram forjados, com a cadeia de certificados forjados sob a confiança da biblioteca Mozilla NSS.

intel Security

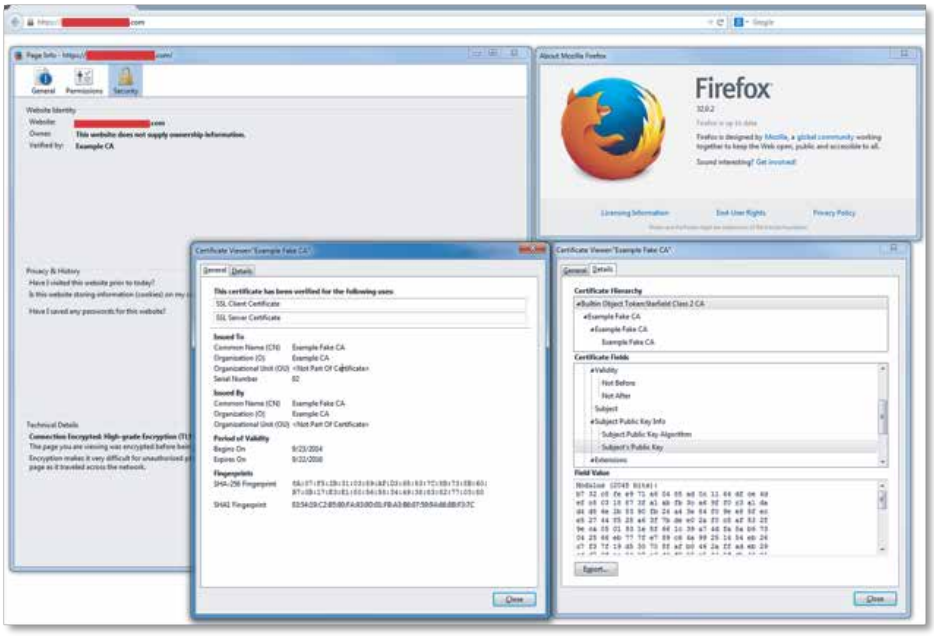

Figura 1. Certificado forjado visto no Firefox.

Como somos afetados pela BERserk? A BERserk e vulnerabilidades relacionadas põem em cheque nossa percepção da confiança e a segurança das sessões que se comunicam por meio de SSL/TLS. Um atacante pode estabelecer uma sessão de intercepção em qualquer tipo de situação com certificados RSA forjados, tornando-o capaz de sequestrar sessões, manipular entradas e saídas ou roubar dados confidenciais.

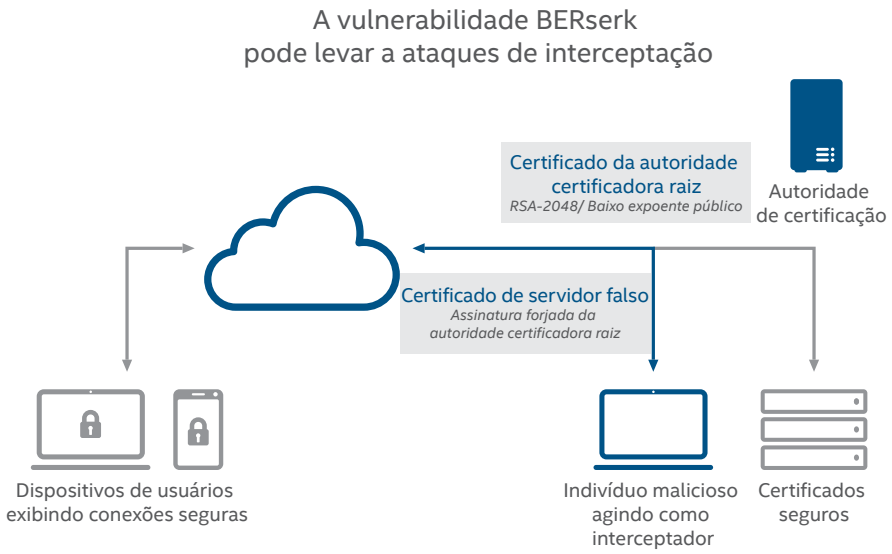

Figura 2. A BERserk permite que os atacantes forjem assinaturas RSA, ignorando, assim, a autenticação a diversos sites.

O que pode ser feito imediatamente?
Certifique-se de que está usando os patches mais recentes da Mozilla para a biblioteca de criptografia Mozilla NSS, para o Firefox, Thunderbird, SeaMonkey e para outros produtos da Mozilla. A Google também lançou patches para o Google Chrome e Chrome OS para remediar o fato de que esses produtos também utilizam a biblioteca vulnerável.

Como a McAfee ajuda na proteção contra a BERserk?

Os produtos da McAfee podem proteger você contra ataques que tentam explorar a vulnerabilidade BERserk. O McAfee Vulnerability Manager faz uma análise completa dos seus sistemas para identificar e informar aqueles que se encontram vulneráveis à BERserk. O McAfee Application Control garante que os aplicativos que estão vulneráveis à BERserk não serão autorizados a ser executados no seu ambiente até serem corrigidos.

McAfee Vulnerability Manager
Ataques como a BERserk ilustram o cenário de ameaças em constante mudança que afeta as empresas hoje em dia. Saber se você está em risco e saber a extensão da sua vulnerabilidade a esses novos ataques pode ser uma tarefa assustadora. Aqui estão algumas formas pelas quais o **McAfee Vulnerability Manager**, junto com o **McAfee Asset Manager**, pode ajudar a sua empresa a compreender vulnerabilidades como a BERserk, e a tomar as medidas necessárias para corrigi-las de forma efetiva:

- **Varredura abrangente de vulnerabilidades:** o McAfee Vulnerability Manager é um produto independente altamente expansível para descoberta de host, gerenciamento de ativos, avaliação de vulnerabilidade e geração de relatórios sobre qualquer dispositivo conectado à rede. O McAfee Vulnerability Manager busca pela BERserk procurando sistemas que estão executando versões vulneráveis do Firefox, Chrome e outros produtos que usam a biblioteca de criptografia Mozilla NSS vulnerável.
- **Personalize varreduras para novas ameaças:** o Foundstone Scripting Language (FSL) Editor pode complementar as verificações predefinidas e atualizações para ameaças de dia zero e vulnerabilidades, como a BERserk, criando verificações e scripts personalizados para avaliar seu ambiente. A partir de 24 de setembro de 2014, o McAfee Vulnerability Manager passa a detectar sistemas vulneráveis à BERserk dentro de suas verificações predefinidas.
- **Geração de relatórios e correção flexíveis:** o McAfee Vulnerability Manager e o McAfee Asset Manager trabalham juntos para oferecer monitoramento automatizado e gerenciamento de varredura, correção, imposição e geração de relatórios. Isso ajuda a evitar demoradas simulações de emergências e processos específicos, a eliminar erros e a proteger mais sistemas de maneira eficiente.
- **Conheça a sua exposição:** o McAfee Asset Manager permite que a sua empresa saiba quais sistemas estão vulneráveis à BERserk pela correlação de varreduras de vulnerabilidade com varreduras de descoberta de host. Poder identificar em tempo real quais sistemas estão executando versões vulneráveis do Firefox e outros aplicativos significa perder menos tempo pensando se você está exposto e poder dedicar mais tempo à correção.

McAfee Application Control
É fundamental proteger sua empresa de códigos e aplicativos indesejados, como aqueles que são vulneráveis à BERserk. O **McAfee Application Control** permite que a sua empresa controle quais aplicativos estão autorizados a ser executados no seu ambiente através de listas brancas dinâmicas e políticas de imposição para endpoints tanto conectados quanto desconectados.

- **Listas brancas dinâmicas:** permitem que sua organização gerencie de forma eficiente os aplicativos relacionados em listas brancas, elaborando tais listas automaticamente conforme os sistemas são corrigidos e atualizados. O McAfee Application Control é capaz de reduzir a sua exposição à BERserk ao impedir a execução de aplicativos que invocam o código vulnerável de verificação de assinatura RSA.
- **Reputação de arquivos:** a integração com o **McAfee Global Threat Intelligence** permite que o McAfee Application Control consulte canais em tempo real de tipos de arquivos válidos conhecidos, inválidos e desconhecidos, ajudando a sua empresa a ficar atenta a novas vulnerabilidades, como a BERserk.
- **Mantenha-se protegido, conectado ou desconectado:** imponha controles a servidores conectados ou desconectados, máquinas virtuais, endpoints e dispositivos fixos, como terminais de ponto de venda.

A BERserk é uma vulnerabilidade grave que pode expor seus sistemas a uma ampla variedade de ataques. As tecnologias de segurança da McAfee são capazes de identificar os sistemas vulneráveis e bloquear os ataques que exploram a BERserk.

Para informações adicionais sobre a BERserk:

- **BERserk vulnerability: Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Vulnerabilidade BERserk: parte 1: ataque por falsificação de assinatura RSA decorrente de análise incorreta de DigestInfo com codificação ASN.1 em PKCS#1 v1.5)
- **BERserk vulnerability: Part 2: Certificate forgery in Mozilla NSS** (Vulnerabilidade BERserk: parte 2: falsificação de certificados na Mozilla NSS)
- Computer Emergency Response Team: **VU#772676**
- National Vulnerability Database: **CVE-2014-1568**
- Blog da McAfee: **http://blogs.mcafee.com/executive-perspectives/need-know-berserk-mozilla**

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com