Panoramica sulla soluzione

BERserk: passare al contrattacco

Per ricominciare a fidarsi della connettività affidabile.

La definizione di fiducia sta cambiando? Attacchi come BERserk e Heartbleed mettono in crisi la buona fede con cui ci affidiamo ai protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS). Non può esservi fiducia quando vengono messe in dubbio la riservatezza, l'integrità e l'autenticità delle nostre informazioni. Come fare per garantire che la vostra azienda sia protetta dall'abuso di fiducia perpetrato da BERserk?

Che cos'è BERserk?

Il **Report McAfee Labs sulle minacce: novembre 2014** contiene un esame approfondito della vulnerabilità BERserk. BERserk è una vulnerabilità insita nelle modalità di verifica delle firme RSA, che permette la contraffazione di tali firme. Per rimediarvi, Mozilla ha rilasciato delle patch per la libreria crittografica Mozilla Network Security Services (NSS), utilizzata comunemente nel browser Firefox ma presente anche in Thunderbird, SeaMonkey, Google Chrome e altri prodotti. BERserk consente ai malintenzionati di sferrare attacchi "man in the middle" (MITM) con la contraffazione delle firme RSA e l'elusione dell'autenticazione ai siti mediante SSL/TLS.

Questa vulnerabilità è una variazione di quella che permette la contraffazione delle firme RSA PKCS#1 v1.5 segnalata da Bleichenbacher e definita nelle **CVE-2006-4339**. La falla è causata dall'analisi errata delle codifiche ASN.1 durante la verifica delle firme, e l'attacco sfrutta il fatto che la lunghezza di un campo nelle regole di codifica di base (BER) permette utilizzare molti byte di dati. Nelle implementazioni vulnerabili, la presenza di molti byte fa sì che questi vengano saltati durante l'analisi.

Questo significa che è possibile falsificare i certificati RSA senza conoscere la chiave privata RSA corrispondente. È stato dimostrato che è possibile contraffare certificati RSA sia a 1024 bit che a 2048 bit, e che la catena dei certificati contraffatti viene considerata affidabile da Mozilla NSS.

intel Security

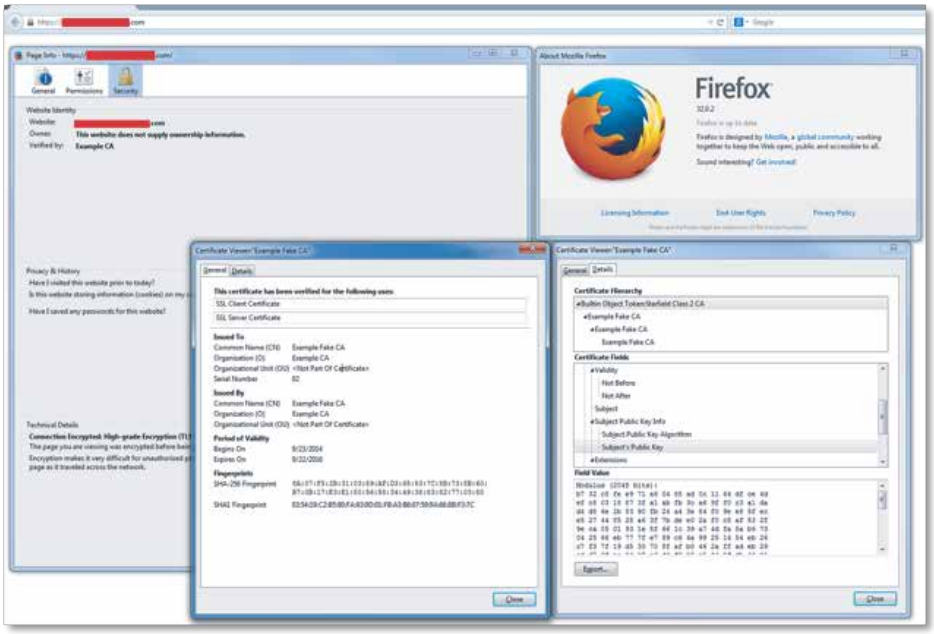

Figura 1. Certificato contraffatto, osservato in Firefox.

Che cosa comporta tutto questo per noi? BERserk e altre vulnerabilità di questo tipo compromettono l'affidabilità e la sicurezza intrinseche delle sessioni che comunicano tramite i protocolli SSL/TLS. Con dei certificati RSA falsificati, un aggressore può instaurare una sessione MITM in un'infinità di situazioni e può così assumere il controllo delle sessioni, manipolare l'input e l'output o sottrarre dati sensibili.

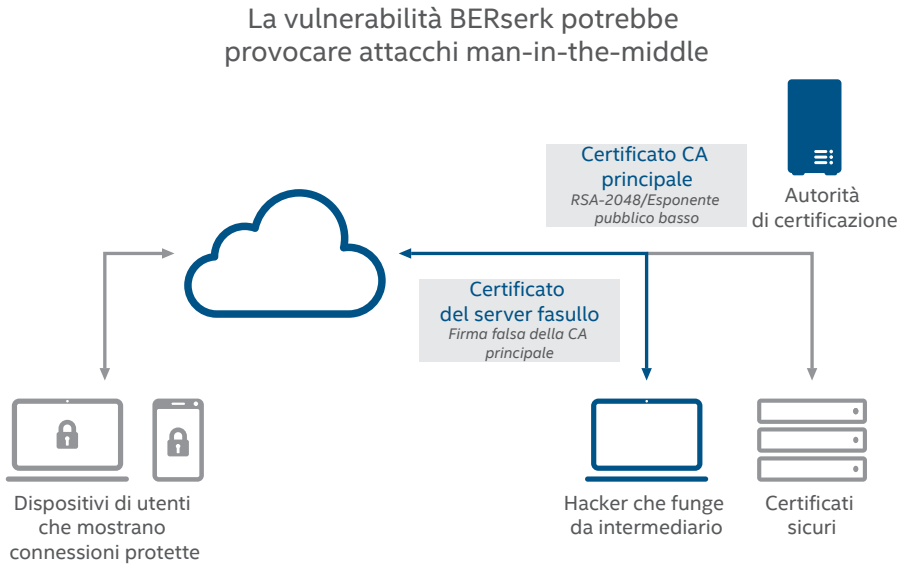

Figura 2. BERserk permette ai malintenzionati di falsificare le firme RSA e di eludere l'autenticazione su numerosi siti Web.

Che cosa si può fare nell'immediato?
Controllate di avere installato le patch più recenti per la libreria crittografica Mozilla NSS, per Firefox, Thunderbird, SeaMonkey e altri prodotti Mozilla. Anche Google ha rilasciato delle patch per Google Chrome e per il sistema operativo Chrome OS, per rimediare al fatto che anche questi prodotti fanno uso della libreria vulnerabile.

Che cosa può fare McAfee per aiutarvi a proteggervi da BERserk?

I prodotti McAfee possono proteggervi dagli attacchi che tentano di sfruttare la vulnerabilità BERserk. McAfee Vulnerability Manager può esaminare i vostri sistemi per identificare e segnalare quelli vulnerabili a BERserk. McAfee Application Control può impedire l'esecuzione delle applicazioni vulnerabili a BERserk nel vostro ambiente fino a quando non siano state corrette.

McAfee Vulnerability Manager
Attacchi come BERserk sono un esempio del panorama delle minacce in costante mutamento con cui le aziende di oggi devono fare i conti. Capire se si è a rischio e fino a che punto si è vulnerabili a questi nuovi attacchi può essere un'impresa ardua. Ecco in che modo **McAfee Vulnerability Manager** e **McAfee Asset Manager** possono aiutare la vostra azienda a capire vulnerabilità come BERserk e ad adottare le misure più efficaci per porvi rimedio:

- **Scansione completa delle vulnerabilità:** McAfee Vulnerability Manager è una soluzione standalone estremamente scalabile per il rilevamento degli host, la gestione delle risorse, la valutazione delle vulnerabilità e la generazione di rapporti su qualsiasi dispositivo connesso alla rete. McAfee Vulnerability Manager può controllare se si è esposti al rischio BERserk cercando sistemi su cui sono installate versioni vulnerabili di Firefox, Chrome e altri prodotti che utilizzano la libreria crittografica Mozilla NSS.
- **Personalizzazione delle scansioni per nuove minacce:** Foundstone Scripting Language (FSL) Editor può amplificare i controlli e gli aggiornamenti predefiniti per le minacce zero-day e le vulnerabilità come BERserk con script e controlli personalizzati per valutare il vostro ambiente. McAfee Vulnerability Manager è ora in grado di rilevare i sistemi vulnerabili a BERserk con i controlli predefiniti aggiornati al 24 settembre 2014.
- **Flessibilità nella generazione di rapporti e nella remediation:** McAfee Vulnerability Manager e McAfee Asset Manager operano in sinergia per garantire il monitoraggio e la gestione automatici delle scansioni, delle attività di remediation e di imposizione e della generazione di rapporti. In questo modo non dovrete perdere tempo a imparare procedure di emergenza e implementare processi ad hoc, eliminerete gli errori e proteggerete efficacemente un maggior numero di sistemi.
- **Conoscenza del grado di esposizione:** McAfee Asset Manager permette all'azienda di sapere quali sono i sistemi vulnerabili a BERserk correlando le scansioni delle vulnerabilità con le scansioni di rilevamento degli host. Identificare in tempo reale i sistemi con versioni vulnerabili di Firefox e di altre applicazioni vi evita di perdere tempo a chiedervi se siete esposti al rischio e vi permette di concentrarvi sugli interventi di remediation.

McAfee Application Control
È di fondamentale importanza proteggere la vostra azienda dal codice e dalle applicazioni indesiderate come quelle vulnerabili a BERserk. **McAfee Application Control** vi permette di controllare le applicazioni di cui è autorizzata l'esecuzione nel vostro ambiente mediante policy di whitelisting dinamico e di imposizione sia sugli endpoint connessi che su quelli offline.

- **Whitelisting dinamico:** consente alla vostra organizzazione di gestire con efficienza le applicazioni presenti nella whitelist, compilandola automaticamente via via che i sistemi vengono aggiornati e dotati di patch. McAfee Application Control può ridurre la vostra esposizione a BERserk impedendo l'esecuzione delle applicazioni che chiamano il codice di verifica delle firme RSA vulnerabile.
- **Reputazione dei file:** l'integrazione con **McAfee Global Threat Intelligence** permette a McAfee Application Control di interrogare flussi di informazioni in tempo reale sui tipi di file noti — innocui, pericolosi e sconosciuti — per mantenere la vostra azienda sempre al corrente delle nuove vulnerabilità come BERserk.
- **Protezione per dispositivi connessi e non connessi:** vengono imposti controlli su tutti i dispositivi, connessi e non connessi: server, macchine virtuali, endpoint e dispositivi fissi come i terminali POS.

BERserk è una vulnerabilità grave che può esporre i vostri sistemi a moltissimi tipi di attacchi diversi. La tecnologia di sicurezza McAfee può identificare i sistemi vulnerabili e bloccare gli attacchi che sfruttano la vulnerabilità BERserk.

Per maggiori informazioni su BERserk:

- **BERserk vulnerability: Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Vulnerabilità BERserk: Parte 1: Attacco con falsificazione di firma RSA dovuto ad analisi errata del DigestInfo codificato con ASN.1 in PKCS#1 v1.5)
- **BERserk vulnerability: Part 2: Certificate forgery in Mozilla NSS** (Vulnerabilità BERserk: Parte 2: Falsificazione di certificati in 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.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com