Краткий обзор решения

Противодействие уязвимости BERserk

Восстановление доверия к защищенным подключениям

Можем ли мы по-прежнему доверять защищенным подключениям? Атаки, подобные BERserk и Heartbleed, пошатнули былую репутацию протоколов Secure Sockets Layer (SSL) и Transport Layer Security (TLS). Когда под сомнением оказываются конфиденциальность, целостность и подлинность данных, о доверии не может быть и речи. Как гарантировано защитить свою компанию от злоупотребления доверием посредством уязвимости BERserk?

Что такое BERserk?

Уязвимость BERserk подробно описана в **отчете McAfee Labs об угрозах за ноябрь 2014 года**. BERserk — это уязвимость, позволяющая подделывать цифровые подписи, основанная на несовершенстве алгоритма проверки подписей RSA. Компания Mozilla уже исправила библиотеку шифрования Mozilla Network Security Services (NSS), которая обычно используется в веб-браузере Firefox, но также может присутствовать и в Thunderbird, SeaMonkey, Google Chrome и других продуктах. Уязвимость BERserk предоставляет злоумышленникам возможность проводить атаки с использованием «незаконного посредника», подделывая электронные подписи RSA и обходя алгоритмы проверки подлинности на веб-сайтах, использующих протоколы SSL/TLS.

BERserk является вариантом обнаруженной ранее уязвимости Bleichenbacher PKCS#1 v1.5, описанной под номером **CVE-2006-4339**, которая позволяет злоумышленникам подделывать цифровые подписи RSA. Уязвимость связана с некорректной синтаксической обработкой закодированных последовательностей стандарта ASN.1 в алгоритме проверки цифровой подписи. Опасность заключается в том, что в соответствии с базовыми правилами кодирования (Basic Encoding Rules — BER) длина поля может содержать больше байтов данных, чем того требует стандарт. В уязвимых реализациях алгоритма лишние байты при синтаксической обработке пропускаются.

Таким образом, для подделки сертификатов RSA атакующему даже не нужно знать соответствующие закрытые ключи RSA. В ходе исследований удалось подделать как 1024-, так и 2048-разрядные сертификаты RSA, при этом цепочки поддельных сертификатов были определены модулем Mozilla NSS как подлинные.

intel Security

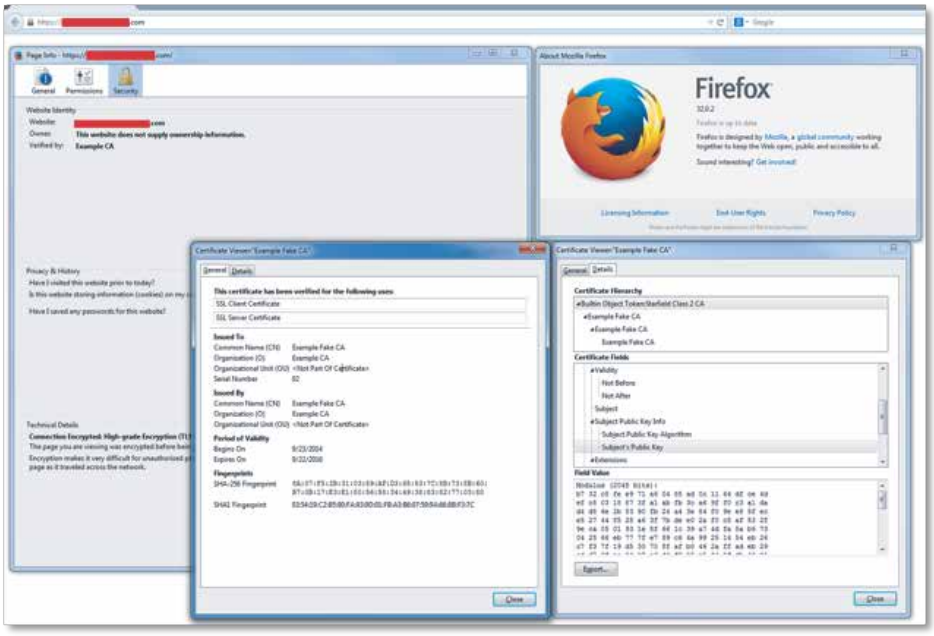

Рис. 1. Поддельный сертификат в Firefox

Чем угрожает нам BERserk? BERserk и другие подобные уязвимости подрывают безопасность и доверие к сеансам связи с использованием протоколов SSL/TLS. Используя поддельные сертификаты RSA, злоумышленники могут создавать сеансы связи с «незаконным посредником» в самых разных сценариях. Это дает им возможность перехватывать сеансы, манипулировать данными ввода/вывода и похищать конфиденциальную информацию.

Рис. 2. Уязвимость BERserk позволяет злоумышленникам подделывать подписи RSA и обходить механизмы проверки подлинности на многих веб-сайтах

Что можно сделать в срочном порядке?
Убедитесь в том, что у вас установлены последние исправления от компании Mozilla для библиотеки шифрования Mozilla NSS, а также для Firefox, Thunderbird, SeaMonkey и других продуктов Mozilla. Аналогичные исправления выпущены компанией Google для браузера Google Chrome и операционной системы Chrome OS, поскольку в этих продуктах тоже используется уязвимая библиотека.

Как McAfee помогает защититься от уязвимости BERserk?

Продукты McAfee способны защитить вас от атак, связанных с попытками использования уязвимости BERserk. McAfee Vulnerability Manager оценивает общее состояние систем и выявляет элементы, подверженные уязвимости BERserk. McAfee Application Control гарантированно предотвращает запуск подверженных уязвимости BERserk приложений в вашей среде до тех пор, пока уязвимость в них не будет устранена.

McAfee Vulnerability Manager
Атаки, подобные BERserk, формируют постоянно меняющийся ландшафт угроз, с которым приходится иметь дело современным предприятиям. Оценка наличия риска и масштабов уязвимости предприятия для этих новых атак может казаться пугающе сложной задачей. Вот лишь некоторые возможности **McAfee Vulnerability Manager** и **McAfee Asset Manager**, использование которых поможет вашей компании выявить уязвимости, подобные BERserk, и принять необходимые меры по эффективному их устранению:

- **Комплексная проверка на наличие уязвимостей.** McAfee Vulnerability Manager — автономное решение с высоким уровнем масштабируемости для обнаружения узлов, управления активами, оценки уязвимостей и составления отчетов обо всех подключенных к сети устройствах. McAfee Vulnerability Manager может выполнять проверку на наличие уязвимости BERserk, анализируя системы, в которых выполняются уязвимые версии Firefox, Chrome и других продуктов, использующих устаревшую библиотеку Mozilla NSS.
- **Настраиваемые алгоритмы проверки для поиска новых угроз.** Редактор сценариев Foundstone Scripting Language (FSL) Editor позволяет расширять набор стандартных проверок и обновлений, необходимых для обнаружения угроз «нулевого дня» и уязвимостей вроде BERserk, путем создания собственных сценариев и правил проверки для оценки вашей среды. Решение McAfee Vulnerability Manager способно обнаруживать системы, подверженные уязвимости BERserk, используя алгоритмы проверки, уже имеющиеся в комплекте поставки по состоянию на 24 сентября 2014 года.
- **Гибкие средства отчетности и устранения уязвимостей.** McAfee Vulnerability Manager и McAfee Asset Manager совместно предоставляют автоматизированные средства мониторинга и управления для проверки, устранения уязвимостей, принудительного соблюдения правил и формирования отчетов. Это позволяет избегать беспорядочных и неорганизованных процессов, отнимающих время, исключает возможные ошибки и повышает эффективность защиты систем.
- **Знание слабых мест.** Сопоставляя результаты поиска уязвимостей с результатами обнаружения узлов, McAfee Asset Manager позволяет определять, какие именно системы предприятия подвержены уязвимости BERserk. Системы, в которых выполняются уязвимые версии Firefox и других приложений, обнаруживаются в режиме реального времени, благодаря чему меньше времени затрачивается на поиск уязвимостей и больше времени остается на их устранение.

McAfee Application Control

Защита предприятия от нежелательного кода и нежелательных приложений, в том числе подверженных уязвимости BERserk, имеет первостепенное значение. **McAfee Application Control** позволяет управлять разрешениями на запуск приложений в среде предприятия при помощи белых списков и политик принудительного соблюдения правил, действующих как на подключенных, так и на не подключенных к сети конечных точках.

- **Динамические белые списки.** Автоматическое создание белых списков приложений при установке исправлений и обновлении систем позволяет организации эффективно управлять разрешениями на запуск приложений. McAfee Application Control снижает подверженность систем уязвимости BERserk, не позволяя выполнять приложения, обращающиеся к коду уязвимого алгоритма проверки цифровых подписей RSA.
- **Репутация файлов.** Интеграция с **McAfee Global Threat Intelligence** дает решению McAfee Application Control возможность в режиме реального времени запрашивать информацию о безопасных, опасных и неизвестных типах файлов, что помогает компании поддерживать осведомленность о новых угрозах вроде BERserk.
- **Защита независимо от наличия подключения к сети.** Обеспечение защиты на подключенных и не подключенных к сети серверах, виртуальных машинах, конечных точках и устройствах с фиксированными функциями, таких как терминалы для приема платежей.

BERserk — это серьезная уязвимость, подвергающая ваши системы широкому спектру угроз. Технологии обеспечения безопасности, разработанные компанией McAfee, позволяют выявлять уязвимые системы и блокировать атаки, использующие уязвимость BERserk.

Дополнительные сведения об уязвимости BERserk можно найти в следующих публикациях.

- **BERserk vulnerability: Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Отчет об уязвимости BERserk: Часть 1. Атака с подделкой цифровых подписей RSA вследствие некорректной синтаксической обработки данных DigestInfo, закодированных по стандарту ASN.1, в PKCS#1 v1.5)
- **BERserk vulnerability: Part 2: Certificate forgery in Mozilla NSS** (Отчет об уязвимости BERserk: Часть 2. Подделка сертификатов в Mozilla NSS)
- Computer Emergency Response Team: **VU#772676**
- National Vulnerability Database: **CVE-2014-1568**
- Блог McAfee: **http://blogs.mcafee.com/executive-perspectives/need-know-berserk-mozilla**

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com