ソリューション概要

BERserkからの保護

信頼された接続の信用を取り戻す

信用の定義が変わるかもしれません。BERserkやHeartbleedなどの攻撃で、SSL（Secure Sockets Layer）とTLS（Transport Layer Security (TLS）が悪用されました。情報の機密性、整合性、信頼性が疑われれば、信用はもはや存在しません。BERserkのような信用の悪用から組織を保護するには、どうすればよいのでしょうか。

BERserkとは

BERserkについては、『**McAfee Labs脅威レポート: 2014年11月**』で詳しく説明しています。BERserkはRSAの署名検証に存在する脆弱性で、これを悪用すると署名の偽造が可能になります。Mozillaは、この脆弱性が存在するMozilla Network Security Services（NSS）暗号化ライブラリにパッチを適用しました。このライブラリはFirefox Webブラウザーで使用されていますが、Thunderbird、SeaMonkey、Google Chromeなどの製品でも使用されている可能性があります。BERserkを悪用してRSA署名を偽装すると、SSL/TLSを使用するWebサイトの認証を回避できるので、様々な仲介者攻撃（MITM）が可能になります。

BERserkは、BleichenbacherのPKCS#1 v1.5 RSA署名偽造の脆弱性（**CVE-2006-4339**）の一種です。署名の検証時にANS.1エンコーディングが正しく解析されないため、基本符号化規則（BER）フィールドで余分なバイトを残すことができます。この脆弱性が存在すると、数バイトのデータで解析が回避される可能性があります。

つまり、対応するRSA秘密鍵を知らなくても、RSA証明書を偽造できることになります。1024バイトと2048バイトのRSA証明書が偽造可能で、偽造した証明書チェーンをMozilla NSSに信頼させることも可能です。

intel Security

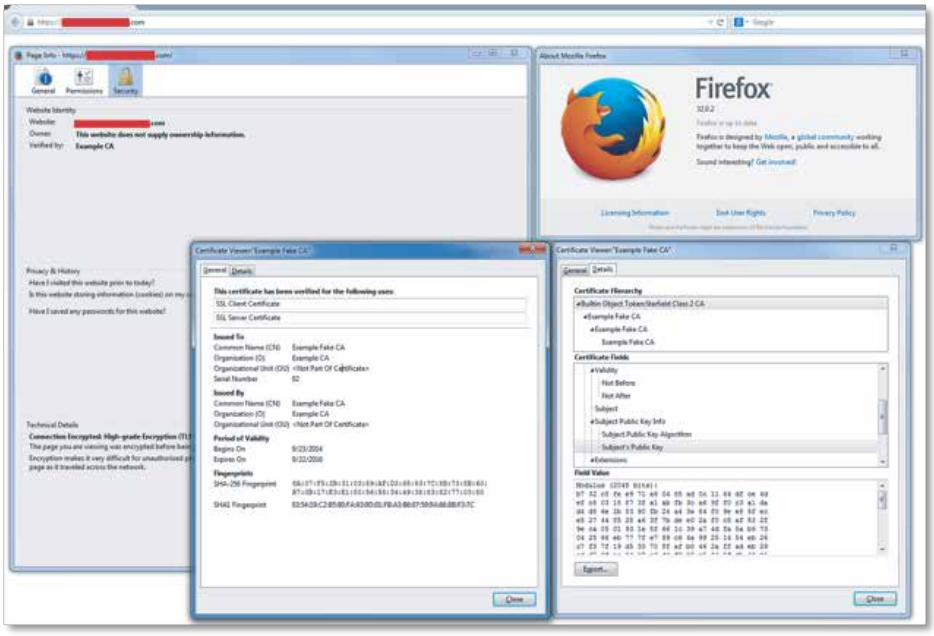

図 1. 偽の証明書をFirefoxで開いたところ。

BERserkでどのような影響を受けるのでしょうか。BERserkや類似した脆弱性は、SSL/TLSを使用したセッションの信頼性とセキュリティに影響を及ぼします。攻撃者は、様々な状況で偽のRSA証明書を使用してMITM攻撃を実行し、セッションの乗っ取り、入出力の操作、重要なデータの窃盗などを行うことができます。

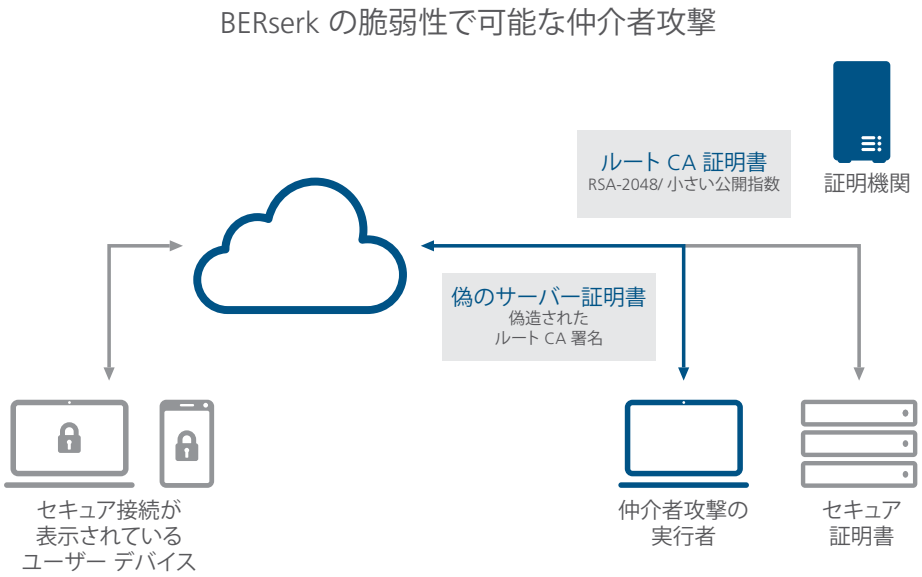

図 2. BERserkの脆弱性を悪用するとRSA署名でWebサイトの認証を回避することも可能

すぐにできる対策は?
MozillaからMozilla NSS暗号化ライブラリ、Firefox、Thunderbird、SeaMonkey、その他のMozilla製品の最新のパッチを入手し、適用する必要があります。Googleも、脆弱なライブラリを使用する製品の問題を解決するため、Google ChromeとChrome OSのパッチをリリースしています。

BERserkに対するマカフィーの対策

マカフィー製品はBERserkの脆弱性を悪用する攻撃を阻止します。McAfee Vulnerability Managerを使用すると、BERserkの脆弱性が存在するシステムを特定できます。McAfee Application Controlを使用すると、BERserkの脆弱性が修正されるまで、この脆弱性が存在するアプリケーションの実行を阻止できます。

McAfee Vulnerability Manager
BERserkのように、信頼モデルの根幹を揺るがす脅威が出現しています。このような新しい攻撃のリスクを把握し、脆弱な範囲を特定することは容易なことではありません。**McAfeeVulnerability Manager**と**McAfee Asset Manager**を使用すると、BERserkなどの脆弱性を迅速に検出し、必要な修復作業を効率的に行うことができます。

- **包括的な脆弱性スキャン:** McAfee Vulnerability Manageは、ホスト検出、資産管理、脆弱性評価を行う拡張性に優れたスタンドアロン製品です。ネットワークに接続しているデバイスに関する報告も行います。McAfee Vulnerability Managerは、脆弱なMozilla NSS暗号化ライブラリを使用するFirefox、Chromeなどの製品が存在するシステムを検出するので、BERserkのリスクも診断できます。
- **新しい脅威に合わせてスキャンをカスタマイズ可能:** Foundstone Scripting Language（FSL）エディターでは、事前に定義された検査を変更することができます。たとえば、ゼロデイ脅威やBERserkなどの脆弱性を検出するように、環境を評価するスクリプトや検査をカスタマイズできます。2014年9月24日の段階で、McAfee Vulnerability Managerの事前定義の検査でBERserkの脆弱性が存在するシステムを検出できます。
- **柔軟なレポートと修復:** McAfee Vulnerability ManagerとMcAfee Asset Managerを使用すると、監視を自動化し、スキャン、修復、施行、レポートなど管理作業を行うことができます。これにより、手間のかかる修復作業や突発的な対応を行う必要がなくなります。エラーが少なくなり、システムをより効率的に保護できます。
- **リスクの把握:** McAfee Asset Managerを使用すると、脆弱性スキャンとホスト検出スキャンを関連付け、BERserkの脆弱性が存在するシステムを特定できます。Firefoxなどのアプリケーションの脆弱なバージョンが存在するシステムをリアルタイムで識別できるので、リスクを迅速に識別し、修復作業を開始できます。

McAfee Application Control
BERserkの脆弱性が存在するアプリケーションや不要なコードから組織を保護する必要があります。**McAfee Application Control**では、動的ホワイトリストとポリシーの施行により、環境内で実行を許可するアプリケーションを制御できます。この機能は、ネットワークに接続していないエンドポイントにも実行できます。

- **動的ホワイトリスト:** システムにパッチが適用され、最新の状態になると、ホワイトリストが自動的に作成されます。これにより、ホワイトリストに登録されたアプリケーションを効率的に管理できます。McAfee Application Controlは、脆弱なRSA署名検証コードを呼び出すアプリケーションの実行を許可しません。このため、BERserkによるリスクを軽減できます。
- **ファイル レピュテーション: McAfee Global Threat Intelligence**の統合により、McAfee Application Controlはファイルの評価情報（正常、不正、不明）をリアルタイムに取得します。BERserkなどの脆弱性を常に監視し、対策を講じることができます。
- **接続状態に関係のない保護:** 接続または切断状態のサーバー、仮想マシン、エンドポイント、POSなどの専用端末を保護します。

BERserkは、様々な攻撃を可能にする重大な脆弱性です。マカフィーのセキュリティ技術は脆弱なシステムを識別し、BERserkを悪用する攻撃をブロックします。

BERserkに関する詳細:

- BERserk vulnerability: **Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5**（BERserkの脆弱性: パート1: PKCS#1 v1.5でASN.1エンコーディングのDigestInfoの解析エラーによるRSA署名偽造攻撃）
- BERserk vulnerability: **Part 2: Certificate forgery in Mozilla NSS**（BERserkの脆弱性: パート2: Mozilla NSSでの証明書の偽装）
- CERT: **VU#772676**
- NVD: **CVE-2014-1568**
- マカフィーのブログ: **http://blogs.mcafee.com/executive-perspectives/need-know-berserk-mozilla**

McAfee. Part of Intel Security.
東京本社　〒150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウエスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内 3-20-17 中外東京海上ビルディング 3F TEL 052-954-9551（代）FAX 052-954-9552
福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com