# セキュリティー報告：BladeCenter Advanced Management Module(AMM)へのOpenSSL脆弱性による影響(CVE-2014-0160 and CVE-2014-0076)

**ヒント集**

【概要】

BladeCenter Advanced Management Module(AMM)で、OpenSSL の脆弱性が発見されました。該当する機能・構成をご利用になる際は対応策を参照・実施ください。

【内容】

CVE ID: CVE-2014-0160

説明：

OpenSSL において、遠隔の攻撃者が、TLS/DTLS ハートビート機能のエラーが原因により、機密情報を取得する可能性があります。攻撃者は、この 脆弱性を利用し、64k の個人メモリー内の情報を閲覧し、秘密鍵を取り出すことが可能です。この攻撃は繰り返し行われる可能性があります。この脆弱性は遠 隔利用が可能であり、認証を必要とせず、簡単に悪用される可能性があります。これは、脆弱な OpenSSL ライブラリを使用して接続を受けた任意のシステ ム（例: サーバー、クライアント、エージェント）に悪用される可能性があります。

CVSS Base Score: 5.0

CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/92322

CVSS Environmental Score*: Undefined

CVSS Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N)

※警告※

ご使用されている環境への潜在的な影響が、CVSS Score で示されているよりもより深刻となる可能性がありますので、できるだけ早く対応を取ることを強くお勧めします。

CVE-ID: CVE-2014-0076

説明：

OpenSSL は ECDSA (Elliptic Curve Digital Signature Algorithm)内の実装エラーが原因で、ローカルの攻撃者が機密情報を入手する可能性があります。

攻撃者は、FLUSH+RELOAD cache side-channel attack to recover ECDSA nonces を使用し、この脆弱性を利用することができます。この脆弱性はローカルでのみ利用可能で、認証を必要とせず、簡単に悪用される可能性がありま す。
CVSS Base Score: 2.1
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/91990
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:L/AC:L/Au:N/C:P/I:N/A:N)

【該当製品とバージョン】
製品

- BladeCenter Advanced Management Module, Option 25R5778
- BladeCenter T Advanced Management Module, Option 32R0835
- BladeCenter(TM)-E: Type 1881, 7967, 8677
- BladeCenter(TM)-H: Types 1886, 7989, 8852
- BladeCenter(TM)-HT: Types 8740, 8750
- BladeCenter(TM)-S: Types 1948, 7779, 8886
- BladeCenter(TM)-T: Types 8720, 8730

Advanced Management Module(AMM)該当ファームウェアバージョン：

- v3.66B (BPET66B)
- v3.66B (BBET66B)
- v3.66B (BPEO66B)
- v3.66C (BPET66C)
- v3.66C (BBET66C)
- v3.66C (BPEO66C)

【対応策】
Lenovo は Fix Central より以下バージョンのファームウェアをダウンロードし、お使いの AMM に適用いただくことを推奨いたします。

Product Version
BladeCenter Advanced Management Module – BladeCenter T Chassis Update to v3.66D (BBET66D)
BladeCenter Advanced Management Module – BladeCenter OEM Chassis Update to v3.66D (BPEO66D)

BladeCenter Advanced Management Module – All other BladeCenter Chassis Update to v3.66D (BPET66D)

ファームウェアの適用後、下記の追加手順が CVE-2014-0160 への対応のために必要です。

1. SSL 証明書の交換

既存の SSL 証明書を無効にし、新しい証明書を再発行する必要があります。古い秘密鍵を使用して新しい証明書を発行せずに、新しい秘密鍵 (例:"openssl genrsa"を使用)を作成する必要があり、新しい秘密鍵を使用し、新たに certificate signing request (CSR)を要求します。

2. ユーザー信用証明書のリセット

OpenSSL の脆弱なバージョンによって保護されたアプリケーションを利用するネットワークユーザーはパスワードを強制的にリセットすべきであり、 OpenSSL がアップグレードされたときより前に設定された認証やクッキーに関するセッションは無効化し、強制的に再認証を行う必要があります。

警告：

お使いの Flex Systems シャーシと他の環境では、Lenovo 製ではない他製品も含めて、追加の修正を必要とする可能性があります。SSL 証明書を交換し、ご使用の環境に必要な修正を適用した後、ユーザーの信用証明書をリセットしてください。

以下は、AMM 上での証明書の交換方法とユーザー信用証明書のリセットに関する具体的な情報です。

証明書交換

証明書再発行についての情報は以下のリンクをご参照ください。

Web interface:

- http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1bb_bc_mmug_mmsecuritypage.html
- https://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1bb_bc_mmug_configldap_secureweb_secureldap.html
- Command line interface:
http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1bc_bc_cli_sslcfg_amm.html

ユーザー信用証明書のリセット

AMM パスワードの変更についての情報は以下をご参照ください。

Web interface:

- http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1bb_bc_mmug_mmloginprofilepage.html
- Command line interface: http://publib.boulder.ibm.com/infocenter/bladectr/documentation/index.jsp?topic=/com.ibm.bladecenter.advmgtmod.doc/kp1bc_bc_cli_users_amm.html

【回避策と緩和策】

None known

【参照】

- Complete CVSS Guide
- On-line Calculator V2
- OpenSSL Project vulnerability website
- Heartbleed

【関連情報】

IBM Secure Engineering Web Portal

IBM Product Security Incident Response Blog

【承認】

なし

【変更履歴】

17 April 2014: Original Copy 発行

＊ CVSS 環境スコアは、お客様の環境固有のもので、最終的には全体の CVSS スコアに影響を与えます。お客様は、このフラッシュのリファレンスセクションのリンクにアクセスすることにより、その環境において、この脆弱性の影響を評価することができます。

注: Forum of Incident Response and Security Teams (FIRST)によると、Common Vulnerability Scoring System (CVSS)は、脆弱性の重要度を伝える、優先度、緊急性を決定するのに役立つよう設計された、業界のオープン標準です。Lenovo は、市場に適した保証の暗 示と特定目的のための適合性を含め、

いかなる種類の保証なしに「現状のまま」、CVSS スコアを提供します。 お客様は、実際のまたは潜在的なセキュリティ脆弱性の影響を評価する責任があります。

以上

※このガイドは、下記サイトを元に作成しています。
<Security Bulletin: BladeCenter Advanced Management Module (AMM) is affected by vulnerabilities in OpenSSL (CVE-2014-0160 and CVE-2014-0076)>
https://www.ibm.com/support/entry/myportal/docdisplay?lndocid=MIGR-5095124