Systems Directorが持つOpenSSL脆弱性への対応について (CVE-2014-0160およびCVE-2014-0076)

2015年4月13日
12:55

Systems Directorが持つOpenSSL脆弱性への対応について (CVE-2014-0160およびCVE-2014-0076) ヒント集

【概要】

Systems Directorが持つOpenSSL脆弱性について、該当するバージョンおよび対応方法を記載しています（System xプラットフォームのWindowsおよびLinux環境）。

お客様環境で稼働しているSystems Directorの環境がこの脆弱性に該当するのか、該当する場合にはどのような対応を行う必要があるのか手順を記載していますので、該当する構成をご利用の場合には本文書に記載の対応策を参照・実施くださいますようお願い申し上げます。

【脆弱性の詳細】

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)

【該当するコンポーネントとバージョン】

・コンポーネント

Systems Director サーバー、共通エージェント、プラットフォーム・エージェント

・バージョン

6.3.2.0、6.3.2.1、6.3.3.0、6.3.3.1

【非該当となる製品のバージョン】

・バージョン

5.2.xx、6.1.x.x、6.2.x.x、6.3.0.0、6.3.1.0、6.3.1.1

※すべてのハードウェア・プラットフォーム上の上記Directorサーバー、Directorエージェントは、OpenSSL Heartbleed脆弱性 (CVE-2014-160) に対しての脆弱性はありません。

【対応策】

Linux上で動作するシステムの場合 Windows上で動作するシステムの場合

■ Linux上で動作するシステムの場合:

プラットフォーム・エージェント、共通エージェントまたはSystems Directorサーバーの共通エージェントがインストールされたシステムに修正パッチを手動でインストールする方法は、以下の通りです。

注意と前提:

- 該当するバージョンが導入されているエンドポイントがあり、アクセスの要求がすでに行われていることを前提とします。
- プラットフォーム・エージェントは、共通エージェント、Systems Directorサーバーにもプログラムの一部として含まれています。
- このパッチは、プラットフォーム・エージェントのOpenSLバイナリがCIMOM通信のために使用されている場合にのみ適用可能です。CIM RSAPがロックされているか、存在しない場合には、使用できません。(共通エージェントCiM RSAPは存在するが、使用されていない場合というのは、ごく限られた影響となります。)
- SSL鍵がリセットされた場合、鍵の長さは2048ビットになり、証明書著名アルゴリズムはSHA256となります。

パッチ必要性の確認:

- このパッチは、プラットフォーム・エージェント バージョン 6.3.2、6.3.2.1、6.3.3、6.3.3.1に対してのみ適用可能です。
- プラットフォーム・エージェント CIMOMは、5989番または代替15989番ポート上のOpenSSLを実行し、エージェントセキュリティー設定のCIM RSAPとして、Systems Director Serverを危険に晒します。
  ※15989番ポートが使用されるケースとしては、OS CIMOMが5989番を使用している場合などです。
- エージェントが影響を受けているか確認するには、以下のコマンドを実行します。
  # /opt/ibm/icc/bin/openssl version

※返されたOpenSSLのバージョンが 1.0.1 の場合、影響を受けることになります。以下の手順を実施ください。

手順:

1. 修正パッチを入手し、OpenSSLのバージョンアップを行う

1.1. 以下のURLからパッチを入手します。ファイルを展開すると、OS、ディストリビューターごとにrpmが用意されていますので、適切なファイルを該当するエンドポイントへ配置します。

・RHEL5_x86 --> ibmcim-ssl-1.0.1-rhel5.i386.rpm

・RHEL6_x86 --> ibmcim-ssl-1.0.1-rhel6.i386.rpm

・SUSE10_x86 --> ibmcim-ssl-1.0.1-sles10.i386.rpm

・SUSE11_x86 --> ibmcim-ssl-1.0.1-sles11.i386.rpm

修正パッチの入手先:

http://www-933.ibm.com/support/fixcentral/systemx/selectFixes?parent=Flex%2BSystem%2BManager%2BNode&product=ibm/systemx/8731&&platform=All&function=fixId&fixids=Flex1_3_1_Platform_Agents_IT00284

1.2. 配置したRPMファイルを使ってインストールします。

```
# rpm -Uvh --force xxxxxxx.rpm
```

例:RHEL6_x86環境の場合には、次のコマンドを実行します。

```
# rpm -Uvh --force ibmcim-ssl-1.0.1-rhel6.i386.rpm
```

1.3. 先述したOpenSSLのバージョンを確認を行うコマンドを実行し、バージョンが更新されていることを確認します。新しいOpenSSLのバージョンは、2014年4月7日付けの1.0.1gです。反映されていれば、パッケージの配置に成功しました。

```
# /opt/ibm/icc/bin/openssl version
```

出力結果例:OpenSSL 1.0.1g 7 Apr 2014

2. 秘密鍵が既に盗用されていると仮定し、SSL暗号化鍵、証明書をリセットする

2.1. 本ステップは必要に応じて実行します。既存の公開鍵を含む証明書情報をダンプする以下のコマンドを実行します。テキストファイルへ出力すると適用前後での比較が容易です。

```
# /opt/ibm/icc/bin/openssl x509 -in $KEYSTORE_PATH/server.cert -noout -text
```

2.2. エンドポイントコマンドを使用して以下のコマンドを実行することにより、変数をセットします。

```
# KEYSTORE_PATH=/etc/opt/ibm/icc/keystore
# ICC_PATH=/opt/ibm/icc
# HOSTNAME=`hostname`
# OPENSSL_CONF=$KEYSTORE_PATH/../openssl.cnf
```

注: hostnameラインの"`"はバッククォーテーションであり、アポストロフィー"'"ではありません。

2.3. 証明書と鍵を再生成します。

```
# echo -e
```

```
"US¥nNORTH CAROLINA¥nRTP¥nIBM¥nSTG¥n$HOSTNAME¥n.¥n.¥n" | $ICC_PATH/bin/openssl req
-x509 -nodes -sha256 -days 3650 -newkey 2048 -config $OPENSSL_CONF
-keyout $KEYSTORE_PATH/server.key -out $KEYSTORE_PATH/server.cert
```

2.4. 新しい証明書と鍵を使用するためにCIMOMを停止、再始動します。

```
# service cimserverd restart
```

2.5. 本ステップは必要に応じて実行します。新しい公開鍵を含む証明書情報をダンプする以下のコマンドを実行します。適用前と比較して変更されていることを確認します。

```
# /opt/ibm/icc/bin/openssl x509 -in $KEYSTORE_PATH/server.cert -noout -text
```

2.6. 本ステップは必要に応じて実行します。CIMOMが新しいSSL証明書で起動、実行しているか確認します。これらのコマンドは、SSL通信 (通常ポートは15989か5989) を使用したCIMOM名前空間(例: root/ibmsd)をリストします。

```
# /opt/ibm/icc/bin/cimcli ns -l <IP_ADDRESS>:<PORT> -s -u <ADMINUSER> -p <PASSWORD>
```

例:

```
# /opt/ibm/icc/bin/cimcli ns -l 192.168.70.100:5989 -s -u root -p password
```

(該当システムのIPアドレスが192.168.70.100、CIMOM通信に使用するポートが5989番、管理者ユーザー名がroot、パスワードがpasswordの場合の例です。)

出力結果例

・失敗例:

```
# /opt/ibm/icc/bin/cimcli ns -l 192.168.10.100:5989 -s -u Administrator -p Passw0rd
Pegasus Exception: Cannot connect to 192.168.10.100:5989. Connection failed. Trying to connect to
192.168.10.100:5989
```

・成功例:

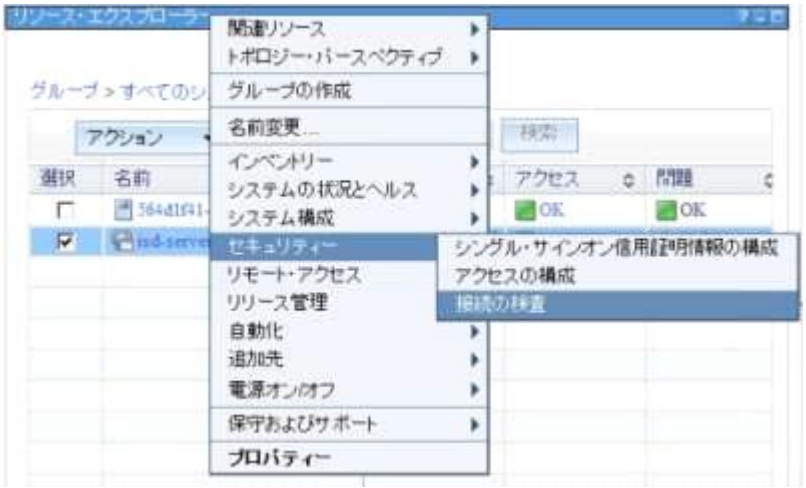
```
# /opt/ibm/icc/bin/cimcli ns -l 192.168.10.100:5989 -s -u Administrator -p Passw0rd
root/subscription
root/subscription/ms_411
root/subscription/ms_409
root/qlogic_cmpi
root/DEFAULT

(中略)

root/emulex
root/brocade
```

<重要> 影響する管理対象システムにアクセス要求で使用されているすべてのユーザーIDは、共通のパスワードを使用して変更されなければなりません。

これは、過去にユーザーがアクセスした際の個人SSL鍵を得ようとする攻撃者から保護するためです。

2.7. 本ステップは必要に応じて実行します。Systems Directorサーバーとプラットフォーム・エージェント管理対象システム間のCIM通信が可能であることを確認します。Systems Directorサーバーでリソース・エクスプローラーを開き、該当管理対象システムを右クリックし、「セキュリティー」→「接続の検査」を開きます。「接続の検査」ボタンを押してアクセスの状態がOKとなれば、管理対象システムとの通信に使用する鍵ストアSSL証明書は機能しています。

注：共通エージェントがインストールされたときのように、CIM RSAPがロックされている、もしくはそこにない場合には、このステップは必要ありません。



以上で対応が完了しました。

■ Windows上で動作するシステムの場合：

プラットフォーム・エージェント、共通エージェントまたはSystems Directorサーバーの共通エージェントがインストールされたシステムに修正パッチを手動でインストールする方法は、以下の通りです。

注意と前提：

- 該当するバージョンが導入されているエンドポイントがあり、アクセスの要求がすでに行われていることを前提とします。
- プラットフォーム・エージェントは、共通エージェント、Systems Directorサーバーにもプログラムの一部として含まれています。
- このパッチは、プラットフォーム・エージェントのOpenSSLバイナリがCIMOM通信のために使用されている場合にのみ適用可能です。CIM RSAPがロックされているか、存在しない場合には、使用できません。（共通エージェントCIM RSAPは存在するが、使用されていない場合というのは、ごく限られた影響となります。）
- SSL鍵がリセットされた場合、鍵の長さは2048ビットになり、証明書著名アルゴリズムはSHA256となります。

パッチ必要性の確認：

- このパッチは、プラットフォーム・エージェント バージョン 6.3.2、6.3.2.1、6.3.3、6.3.3.1に対してのみ適用可能です。
- プラットフォーム・エージェント CIMOMは、5989番または代替15989番ポート上のOpenSSLを実行し、エージェ

ントセキュリティー設定のCIM RSAPとして、Systems Director Serverを危険に晒します。
※15989番ポートが使用されるケースとしては、OS CIMOMが5989番を使用している場合などです。

- エージェントが影響を受けているかを確認するには、コマンド プロンプトから以下のコマンドを実行します。

64bit版 Windowsの場合

```
> "C:¥Program Files (x86)¥Common Files¥ibm¥icc¥cimom¥bin¥openssl.exe" version
```

32bit版 Windowsの場合

```
> "C:¥Proram Files¥Common Files¥ibm¥icc¥cimom¥bin¥openssl.exe" version
```

※返されたOpenSSLのバージョンが 1.0.1 の場合、影響を受けることになります。以下の手順を実施ください。

手順:

1. 修正パッチを入手し、OpenSSLのバージョンアップを行う

1.1. 修正パッチを以下のURLから入手し、影響を受けたシステムへ配置します。

http://www-933.ibm.com/support/fixcentral/systemx/selectFixes?parent=Flex%2BSystem%2BManager%2BNode&product=ibm/systemx/8731&&platform=All&function=fixId&fixids=Flex1_3_1_Platform_Agents_IT00284

1.2. ファイルを展開し、msiインストーラーを実行します。インストール・ウィザードに従って導入が完了しますと再起動を促されますので、再起動を行います。

1.3. 先述したOpenSSLのバージョンを確認を行うコマンドを実行し、バージョンが更新されていることを確認します。新しいOpenSSLのバージョンは、2014年4月7日付けの1.0.1gです。反映されていれば、パッケージの配置に成功しました。

64bit版Windowsの場合

> ″C:¥Program Files (x86)¥Common Files¥ibm¥icc¥cimom¥bin¥openssl.exe″ version

32bit版 Windowsの場合

> ″C:¥Proram Files¥Common Files¥ibm¥icc¥cimom¥bin¥openssl.exe″ version

出力結果例：OpenSSL 1.0.1g 7 Apr 2014

2. 秘密鍵が既に盗用されていると仮定し、SSL暗号化鍵、証明書をリセットする

2.1. コマンド プロンプトを起動しシステム上のプラットフォーム・エージェントCIMOMサブエージェント・プロセスが停止します。以下のコマンドを実行します。

> net stop wmicimserver

2.2. 鍵ストアファイルの存在するディレクトリーへ移動し、「wmicimserver.key」および「wmicimserver.cert」ファイルが存在することを確認します。

64bit版 Windowsの場合

> cd C:¥Program Files (x86)¥Common Files¥ibm¥icc¥cimom¥data¥keystore¥
> dir

32bit版 Windowsの場合

> cd C:¥Program Files¥Common Files¥ibm¥icc¥cimom¥data¥keystore¥
> dir

2.3. ステップは必要に応じて実行します。既存の公開鍵を含む証明書情報を確認するため、コマンド プロンプトから以下のコマンドを実行します。

テキストファイルへ出力すると適用前後での比較が容易です。

> ..¥..¥bin¥openssl.exe x509 -text -noout -in wmicimserver.cert

2.4. 証明書と鍵ファイルである「wmicimserver.key」および「wmicimserver.cert」を新しく作成するため、既存のこれらのファイルをバックアップ用として名前の変更を行いま
す。「wmicimserver.key.old」、「wmicimesrver.cert.old」などに変更します。

2.5. 新しい証明書と鍵を生成します。コマンド プロンプトで ステップ2.2 のディレクトリーに移動し、以下のコマンドを実行します。

```
> ..¥..¥bin¥openssl.exe req -x509 -nodes -sha256 -days 3650 -newkey 2048 -config ..¥..¥bin¥openssl.cnf -keyout wimcimserver.key -out wmicimserver.cert
```

コマンドの実行が進行する中で入力を求めるプロンプトが表示されますので、以下の通り情報を入力します。

```
Country Name (2 letter code) []:US
State or Province Name (full name) []:NORTH CAROLINA
Locality Name (eg, city) []:RTP
Organization Name (eg, company) []:IBM
Organizational Unit Name (eg, section) []:xSeries
Common Name (eg, your websites domain name) []: %machine_hostname% ※エンドポイントの完全修飾ホスト名です。
Email Address []: ※空欄のままEnterを押します。
```

2.6. ステップ2.1 で停止したプラットフォーム・エージェントCIMOMサブエージェント・プロセスを再開します。以下のコマンドを実行します。

```
> net start wmicimserver
```

2.7. 本ステップは必要に応じて実行します。新しい証明書が配置されたことを確認するため、コマンド プロンプトから以下のコマンドを実行します。適用前と比較して変更されていることを確認します。

```
> ..¥..¥bin¥openssl.exe x509 -text -noout -in wmicimserver.cert
```

2.8. 本ステップは必要に応じて実行します。CIMOMが新しいSSL証明書で起動、実行しているか確認します。ここで実行するコマンドは、SSL通信を使用したCIMOM名前空間 (root/ibmsdなど) を画面出力するものです。

```
> cimcli ns -l <IP_ADDRESS>:<PORT> -s -u <ADMINUSER> -p <PASSWORD>
```

例:

cimcli ns -l 192.168.70.100:5989 -s -u Administrator -p Passw0rd

(該当システムのIPアドレスが192.168.70.100、CIMOM通信に使用するポートが5989番、管理者ユーザー名がAdministrator、パスワードがPassw0rdの場合です。)

出力結果例

・失敗例:

```
> cimcli ns -l 192.168.10.100:5989 -s -u Administrator -p Passw0rd
Pegasus Exception: Cannot connect to 192.168.10.100:5989. Connection failed. Trying to connect to
192.168.10.100:5989
```

・成功例:

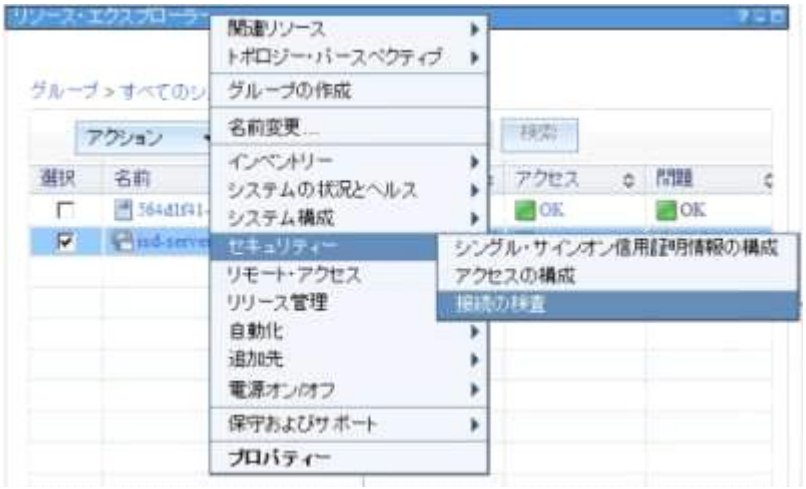
```
> cimcli ns -l 192.168.10.100:5989 -s -u Administrator -p Passw0rd
root/subscription
root/subscription/ms_411
root/subscription/ms_409
root/qlogic_cmpi
root/DEFAULT

(中略)

root/emulex
root/brocade
```

<重要> 影響する管理対象システムにアクセス要求で使用されているすべてのユーザーIDは、共通のパスワードを使用して変更されなければなりません。

これは、過去にユーザーがアクセスした際の個人SSL鍵を得ようとする攻撃者から保護するためです。

2.9. 本ステップは必要に応じて実行します。Systems Directorサーバーとプラットフォーム・エージェント管理対象システム間のCIM通信が可能であることを確認します。Systems Directorサーバーでリソース・エクスプローラーを開き、該当管理対象システムを右クリックし、「セキュリティー」→「接続の検査」を開きます。「接続の検査」ボタンを押してアクセスの状態がOKとなれば、管理対象システムとの通信に使用する鍵ストアSSL証明書は機能しています。

注:共通エージェントがインストールされたときのように、CIM RSAPがロックされている、もしくはそこにない場合には、このステップは必要ありません。



以上で対応が完了しました。

当文書は下記の技術文書をもとに作成しました。

Security Bulletin: Systems Director is affected by vulnerabilities in OpenSSL (CVE-2014-0160 and CVE-2014-0076)

https://www.ibm.com/support/entry/myportal/docdisplay?lndocid=MIGR-5095216

文書番号: SYJ0-ISDHBLEED

最終更新日: 2014-05-12