Empowered by Innovation NEC

Open SSL脆弱性問題(JVN#61247051)の各製品への影響に関して
（データ系ネットワーク製品）
～ Change Cipher Specメッセージ処理の脆弱性 ～

1.0版　2014.06.24

日本電気株式会社
企業ネットワーク事業部

～ JVN(Japan Vulnerability Notesの掲載情報より引用～

＜改版履歴＞

版数	日付	関連項	記事
1.0	2014/06/24	-	初版発行

OpenSSL【オープンSSL】

インターネット上で標準的に利用される暗号通信プロトコルであるSSLおよびTLSの機能を実装した、オープンソースのライブラリ(プログラム部品)。

1. Open SSL脆弱性問題とは？(JVN#61247051)

＜概要＞

2014年6月6日（6月9日更新）に、以下のような
OpenSSL の脆弱性に関する注意喚起が公開されました。

最初の SSL/TLS ハンドシェイクでは、暗号化通信で使われる暗号化鍵を生成するために鍵情報の交換を行い、それに続き Change Cipher Spec メッセージがサーバからクライアントへ、クライアントからサーバへ送られます。
OpenSSL には、Change Cipher Spec プロトコルの実装に問題があり、鍵情報の交換の前に Change Cipher Spec メッセージを受け取ると、空の鍵情報を使って暗号化鍵を生成してしまいます。

http://jvn.jp/jp/JVN61247051/index.html

～ JVN(Japan Vulnerability Notesの掲載情報より引用～

2014-06-06（新規） 2014-06-09（更新）

サーバとクライアント間の SSL/TLS 通信が、
中間者攻撃 (man-in-the-middle attack) によって解読されたり、
改ざんされたりする可能性があります。

2. Open SSL脆弱性問題への対処

本脆弱性問題の影響を受けるバージョンは、以下となります。

サーバ側:

■OpenSSL 1.0.1 系列のうち OpenSSL 1.0.1g およびそれ以前

クライアント側:

■OpenSSL 1.0.1 系列のうち 1.0.1g およびそれ以前
■OpenSSL 1.0.0 系列のうち 1.0.0l およびそれ以前
■OpenSSL 0.9.8 系列のうち 0.9.8y およびそれ以前

本資料では、企業ネットワーク事業部のデータ系ネットワーク製品において、
本脆弱性の該当の有無と該当する場合の対処方法について説明しております。
（弊社製品以外の製品については各メーカーからの情報をご参照ください。）

影響を受ける製品を、ご利用頂いているお客様へご説明および対処をご検討して頂くようにお願いいたします。

3-1. OpenSSL脆弱性(JVN#61247051)に該当する製品一覧(その1)

製品名	対象	詳細情報
UNIVERGE IXシリーズ	Ver. 8.2.19～8.11.11B	詳細は、以下のURLをご参照ください。 http://jpn.nec.com/univerge/ix/Support/CERT/JVN61247051.html
UNIVERGE PFシリーズ	PF5240/PF5248/PF5220 (全バージョン) ※PF6800、PF5459、PF5820は該当しません	SecureChannelでTLS機能を使用している場合に影響あり。(PF6800との接続では未使用のため問題なし) PF52xx : V6.0 (2014/07予定)で対応
UNIVERGE QXシリーズ	該当機種を調査中	
UNIVERGE SG3000LJ UNIVERGE SG3000LG	全バージョン)	詳細は以下のURLをご参照ください。 https://www.support.nec.co.jp/View.aspx?id=3150107549

3-1. OpenSSL脆弱性(JVN#61247051)に該当する製品一覧(その2)

製品名	対象	詳細情報
UNIVERGE UnifiedWall	Check Point R76 Check Point R71.10、R71.40、R71.50	下記の通信が影響を受ける恐れがあります。 1. Mobile Access (SSL-VPN) 利用時の UnifiedWall と接続先の Web サーバ間の通信で下記条件を満たすもの a. Mobile Access (SSL-VPN) ポータル (※1) を利用している場合 b. UnifiedWall と Web サーバ間の通信に HTTPS を利用している場合 c. Web サーバが脆弱性を含む OpenSSL (※2) を使用している場合 2. DynamicID (※3) 利用時の UnifiedWall と SMS プロバイダ間の通信で下記条件を満たすもの d. Mobile Access (SSL-VPN) にて DynamicID を利用している場合 e. SMS プロバイダのサーバが脆弱性を含む OpenSSL (※2) を使用している場合 (注釈) ※1 Web ブラウザベースでの SSL-VPN アクセス。 ※2 OpenSSL のバージョン番号 1.0.1～1.0.1g のみ。 ※3 SMS を利用した2要素認証機能。 対処方法等については以下のURLをご参照ください。(ログインが必要です) https://www.support.nec.co.jp/View.aspx?id=3150107560
UNIVERGE WAシリーズ	Ver. 4.2.3～5.1.3	詳細は、以下のURLをご参照ください。 http://jpn.nec.com/univerge/wa/info/openssl.html

3-2. OpenSSL脆弱性(JVN#61247051)に該当しない製品一覧

製品名	対象	詳細情報
UNIVERGE IP8800シリーズ	ー	
UNIVERGE SecureBranch Eシリーズ	ー	
UNIVERGE SecureBranch SOHO	ー	
UNIVERGE WanBooster	ー	