Empowered by Innovation NEC

Open SSL脆弱性問題の
各製品への影響に関して
(JVN#61247051)
～ Change Cipher Specメッセージ処理の脆弱性 ～

1.0版　2014.06.18

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	2014/06/18	-	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各製品において、
下記の観点でまとめております。

- 上記バージョンのOpenSSLを使用しているかいないか？
- 使用している場合、その対処はどうすれば良いか？

影響を受ける製品を、ご利用頂いている場合、
ご購入いただいたNEC営業拠点・販売店に、ご相談をお願いいたします。

3-1. 音声系本体関連

製品名	OpenSSL 使用有無	動作影響		対処計画
UNIVERGE SV9500	有	無	(該当バージョン未使用)	
UNIVERGE SV8500	有	無	(該当バージョン未使用)	
UNIVERGE SV7000	有	無	(該当バージョン未使用)	
UNIVERGE APEX7600i	無	無	－	
UNIVERGE SV9300	無	無	－	
UNIVERGE SV8300	無	無	－	
UNIVERGE APEX3600i	無	無	－	
SV93 PCPro	無	無	－	
SV83 PCPro	無	無	－	
UNIVERGE MA4000	無	無	－	
IPMASTER-104xAシリーズ	無	無	－	
CALL REGISTER 1000	無	無	－	
PC中継台関連	無	無	－	
NEPARC関連	無	無	－	
SMDR(課金装置)	無	無	－	

3-2. UNIVERGE 3C

製品名	OpenSSL 使用有無	動作影響		対処計画
3C / UCM 次のコンポーネントを含む。 ・UC Client for Windows and MAC OS ・3C Web Administration ・3C Administration application ・NEC VG3 media gateway	有	有		パッチをリリース予定(別途通知)
3C / CMM	有	(有)		Ubuntu OSをバージョンアップして頂く必要があります。 (Ubuntu OSが使用)
3C Connect Outlook add-in	無	無	–	
3C Collaboration client for iOS	無	無	–	
3C Mobile Client for iOS	無	無	–	
Mobile Client for Android	無	(有)		Android OSをバージョンアップして頂く必要があります。 (Android OSが使用)

3-3. アプリケーション(1/2)

製品名	OpenSSL 使用有無	動作影響		対処計画
UNIVERGE ケータイポータル	有	無	(該当バージョン未使用)	
UNIVERGE OW5000	無	無	ー	
UNIVERGE UC700/MC550	無	無	ー	
UNIVERGE Business ConneCT	有	無	(リリース機能に影響無)	
UNIVERGE ActivePhoneBook	有	無	(該当バージョン未使用)	
ダイヤル・アシスタント	無	無	ー	

3-3. アプリケーション(2/2)

製品名	OpenSSL 使用有無	動作影響		対処計画
UNIVERGE ST450	有	有		実装しているOpenSSLを対策版に変更し、動作確認後、AppStoreへ掲載予定。
UNIVERGE ST465	無	無	－	
UNIVERGE Soft Client SP350	有	無	(リリース機能に影響無)	
DtermSP30	有	無	(リリース機能に影響無)	
Star Office21/電子電話帳	無	無	－	
OAI Library for Windows Development Kit	無	無	－	
メッセージ送信システム	無	無	－	
OfficeCollaborator	無	無	－	

3-4. ボイスメール関連

製品名	OpenSSL 使用有無	動作影響		対処計画
UNIVERGE UM8000	有	無	(該当バージョン未使用)	
UnifiedStar i Standard	無	無	–	
UnifiedStar i Professional	無	無	–	
UnifiedStar i Compact	無	無	–	
UnifiedStar Excellent	無	無	–	
たっち録EX	無	無	–	
たっち録Jr	無	無	–	

3-5. コンタクトセンター関連

製品名	OpenSSL 使用有無	動作影響		対処計画
UNIVERGE ContactCenter Manager	無	無	–	
UNIVERGE ContactCenter Integrator	無	無	–	
UNIVERGE ContactCenter Reporter	無	無	–	
UNIVERGE ContactCenter Auditor	無	無	–	
CTIPRO-EX	無	無	–	
NAVIGATORMIS	無	無	–	
@Log	無	無	–	

3-6. 固定電話機関連(1/2)

製品名	OpenSSL 使用有無	動作影響		対処計画
DT400	無	無	-	
DT300	無	無	-	
Dterm85	無	無	-	
Dterm70/75	無	無	-	
DT800	有	無	(該当バージョン未使用)	
DT700(DT770Gを除く)	有	無	(該当バージョン未使用)	
DT770G	有	無	(該当バージョン未使用)	
IPterm85(32D/8D)	有	無	(該当バージョン未使用)	
IPterm85(32K)	有	無	(該当バージョン未使用)	
IPtermSIP85	有	無	(該当バージョン未使用)	
Dterm85(IP)	有	無	(該当バージョン未使用)	
Dterm75(IP)	無	無	-	
NEterm50/60	有	無	(該当バージョン未使用)	

3-6. 固定電話機関連(2/2)

製品名	OpenSSL 使用有無	動作影響		対処計画
Dterm25/αポチ/シェルティ	無	無	-	
DT250	無	無	-	
DT210	無	無	-	

3-7. その他

製品名	OpenSSL 使用有無	動作影響		対処計画
UNIVERGE RD1000	無	有	製品としては、非該当 動作させるOS側の機能に関連し、利用OSとして RHEL5、RHEL6が選択されている場合のみ該当。 対策版のOpenSSLとの組み合わせでご利用ください。	
UNIVERGE WLシリーズ	有	有		(対応方針を検討中)
UNIVERGE SecureBranch	有	無	(該当バージョン未使用)	