Empowered by Innovation NEC

Open SSL脆弱性問題の各製品への影響に関して (JVNVU#94401838)

～ heartbeat 拡張 情報漏えいの脆弱性 ～

4.0版　2014.06.11

日本電気株式会社
企業ネットワーク事業部

～JPCERTコーディネーションセンター（JPCERT/CC）の掲載情報より引用～

1. Open SSL脆弱性問題とは？

＜概要＞

2014年4月8日(4月11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。

OpenSSL Project が提供する OpenSSL の heartbeat 拡張には
情報漏えいの 脆弱性があります。結果として、遠隔の第三者は、細工した
パケットを送付す ることでシステムのメモリ内の情報を閲覧し、秘密鍵などの
重要な情報を取得 する可能性があります。

https://www.jpcert.or.jp/at/2014/at140013.html

～JPCERTコーディネーションセンター（JPCERT/CC）の掲載情報より引用～
2014-04-08(新規) 2014-04-11(更新)

**リモートの攻撃者によって、
秘密鍵等の重要な情報が漏洩する可能性があります。**

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)。

Empowered by Innovation NEC

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。

- OpenSSL 1.0.1 から 1.0.1f
- OpenSSL 1.0.2-beta から 1.0.2-beta1

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。

Empowered by Innovation NEC

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	－	

Empowered by Innovation NEC

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	以下のバージョンが影響有 V8.5.1.x V8.5.2.x (JITC/LSC版) V8.5.3.x	パッチをリリース
3C / CMM	有	無	(該当バージョン未使用)	
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)	Androideの SSL/TLS ライブラリを使っており、Android OS V4.1.1 は影響あると Googleは発表。Android OSをバージョンアップして頂く必要があります。	

Empowered by Innovation NEC

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	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、V5のみ注意。 ・V4(RHEL5)：非該当（openssl-0.9.8e） ・V5(RHEL6)：利用OSとしてRHEL6.5が選択されている場合のみ該当(openssl-1.0.1がOS上で採用されてるため)、それ以外は非該当(openssl-1.0.0) RHEL6.5の環境で、OpenSSLを対策版(openssl-1.0.1e-16.el6_5.7.i686)にUpdateして動作確認済み。
UNIVERGE OW5000	無	無	ー	
UNIVERGE UC700/MC550	無	無	ー	
UNIVERGE Business ConneCT	有	無	(該当バージョン未使用)	
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	

Empowered by Innovation NEC

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	該当バージョン使用	実装しているOpenSSLをVer1.0.1gに変更し、動作確認後、AppStoreへ掲載済(5/9)。
UNIVERGE ST465	無	無	－	
UNIVERGE Soft Client SP350	有	無	(該当バージョン未使用)	
DtermSP30	有	無	(該当バージョン未使用)	
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	－	

Empowered by Innovation NEC

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	ー	
UnifiedStar i Professional	無	無	ー	
UnifiedStar i Compact	無	無	ー	
UnifiedStar Excellent	無	無	ー	
たっち録EX	無	無	ー	
たっち録Jr	無	無	ー	

Empowered by Innovation NEC

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	–	

Empowered by Innovation NEC

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)	

Empowered by Innovation NEC

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	-	

Empowered by Innovation NEC

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 RHEL6.5が選択されている場合のみ該当。 新版のOpenSSLとの組み合わせで、動作確認を実施し 正常動作を確認済	
UNIVERGE WLシリーズ	有	無	(該当バージョン未使用)	
UNIVERGE SecureBranch	有	無	(該当バージョン未使用)	

Empowered by Innovation NEC