Empowered by Innovation NEC

OpenSSL脆弱性問題の各製品への影響に関して（データ系ネットワーク製品）

1.0版　2014.05.15

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～

＜改版履歴＞

版数	日付	関連項	記事
1.0	2014/05/15	-	初版発行

1. OpenSSL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（CVE-2014-0160）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)。

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データ系ネットワーク製品において、
本脆弱性(CVE-2014-0160)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(CVE-2014-0160)に該当する製品一覧

製品名	対象	詳細情報
UNIVERGE PFシリーズ	PF5240/PF5248/PF5220 (V5.1.1.0, V5.1.1.1) ※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があります。(PF6800との接続では未使用のため問題はありません) PF52xx : V6.0 (2014/07予定)で対応
UNIVERGE ThreatDefender	Ver.6.3.4.0 Hotfix 12.2 (Hotfix 12.1以下は影響なし)	脆弱性の問題に対応した、Hotfixを適用してください。 1. 対象製品 UNIVERGE ThreatDefender 100/500/1000 UNIVERGE ThreatDefender Enterprise Manager-05/10 対象バージョン: 6.3.4.0 Hotfix 12.2 なお、Hotfix 12.1 以下は古い OpenSSL を使用しているため脆弱性の影響はありません。 2. パッチ適用方法 以下のURLを参照し、パッチを適用してください。(保守契約が必要です) http://www.support.nec.co.jp/View.aspx?id=9010103179

3-2. OpenSSL脆弱性(CVE-2014-0160)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 IXシリーズ	ー	
UNIVERGE QXシリーズ	ー	
UNIVERGE SecureBranch Eシリーズ	ー	
UNIVERGE SecureBranch SOHO	ー	
UNIVERGE SG3000LJ	ー	
UNIVERGE SG3000LG	ー	
UNIVERGE UnifiedWall	ー	
UNIVERGE WAシリーズ	ー	
UNIVERGE WanBooster	ー	