TD61-5837
HCVU000000014
2014 年 7 月 3 日
日立金属株式会社
電線材料カンパニー
情報システム統括部

OpenSSL に関する複数の脆弱性(VU#978508 他)

1．脆弱性の概要

OpenSSL Project の下記のリンクにおいて、複数の脆弱性情報が公開されています。
(CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-0198, CVE-2010-5298, CVE-2014-3470)
https://www.openssl.org/news/secadv_20140605.txt

2．参考情報

(1) CVE-2014-0224
OpenSSL における Change Cipher Spec メッセージの処理に脆弱性
http://jvn.jp/jp/JVN61247051/index.html

(2) CVE-2014-0221
OpenSSL の d1_both.c の dtls1_get_message_fragment 関数におけるサービス運用妨害 (DoS) の脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-002766.html

(3) CVE-2014-0195
OpenSSL の d1_both.c の dtls1_reassemble_fragment 関数における任意のコードを実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-002765.html

(4) CVE-2014-0198
OpenSSL の s3_pkt.c 内の do_ssl3_write 関数におけるサービス運用妨害 (DoS) の脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-002392.html

(5) CVE-2010-5298
OpenSSL の s3_pkt.c の ssl3_read_bytes 関数におけるセッション間でデータを挿入される脆弱性
http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-005667.html

(6) CVE-2014-3470
OpenSSL の s3_clnt.c の ssl3_send_client_key_exchange 関数におけるサービス運用妨害 (DoS) の脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-002767.html

3．当社製品への影響

当社製品の本脆弱性に関する影響は下記の通りです。

表1 ネットワーク装置

製品名	OS 名称	影響
Apresia26000 シリーズ	AMIOS6	(1)～(6)全て該当しません。
Apresia18000 シリーズ	AMIOS2	
Apresia16000 シリーズ	AMIOS3	
Apresia12000 シリーズ	AMIOS5	
Apresia8000 シリーズ	ApWare	
Apresia6000 シリーズ	ApbWare	
Apresia13000,15000 シリーズ	AEOS8	
Apresia3000,4000, 5000,13000 シリーズ	AEOS7,AEOS6	
ApresiaLight FM シリーズ	APLFMOS	
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLight シリーズ	APL-Ware	
XLGMC シリーズ	-	
XGMC シリーズ	-	
GMC シリーズ	-	
GMX シリーズ	-	
eWAVE シリーズ	-	
BMC シリーズ	-	
GMA シリーズ	-	

表2 ネットワーク管理システム

ソフトウェア名	影響
HCL Manager Station	(1)～(6)全て該当しません。
ApresiaManager	
MMRPManager	
Command Navigator	
ApresiaManager/C	
GMXManager	
GMAManager	
BMCManager	
OSWManager	
OAM-LB Navigator	
BFSManager	

4．回避策

特に必要ありません。

以上