TD61-6675
HCVU000000023
2018 年 1 月 15 日
APRESIA Systems 株式会社
ネットワーク事業本部

CPU に対するサイドチャネル攻撃について(JVNVU#93823979)

1. 脆弱性の概要

投機的実行機能やアウトオブオーダー実行機能を持つ CPU に対してサイドチャネル攻撃の手法が報告されています。以下の手法を用いることにより、保護されているメモリー領域に格納された情報が不正に取得される可能性があります。

(1) データキャッシュを不正に読み取ることにより情報を取得する手法[Meltdown] (CVE-2017-5754)
(2) メモリーの境界チェックを迂回する手法[Spectre 1] (CVE-2017-5753)
(3) CPU の予測分岐機能を悪用する手法[Spectre 2] (CVE-2017-5715)

2. 参考情報

CPU に対するサイドチャネル攻撃
http://jvn.jp/vu/JVNVU93823979/

3. 当社製品への影響

当社製品の本脆弱性に関する影響を下表に示します。

一部の装置では投機的実行機能を持つ CPU を搭載しています。ただし、該当装置において不正に情報を取得するソフトウェアを実行することはできないため、影響はありません。

表 1 ネットワーク装置

製品名	OS 名称	影響
Apresia26000 シリーズ(QC 含む)	AMIOS6	本脆弱性による影響はありません。
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	
Apresia2000,3000,4000, 5000,13000 シリーズ	AEOS7,AEOS6	
ApresiaNP7000 シリーズ	AEOS-NP7000	
ApresiaNP5000 シリーズ	AEOS-NP5000	
ApresiaNP2000 シリーズ	AEOS-NP2000	
ApresiaLight FM シリーズ	APLFMOS	
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLightGM152	APLGM152OS	
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
ANRC シリーズ	本脆弱性による影響はありません。
HCL Manager Station	
ApresiaManager	
MMRPManager	
Command Navigator	
ApresiaManager/C	
GMXManager	
GMAManager	
BMCManager	
OSWManager	
OAM-LB Navigator	
BFSManager	

4. 回避策

必要ありません。

以上