

## ApresiaNPシリーズSSHサーバー機能の脆弱性

### 1. 概要

ApresiaNPシリーズには、不正な情報を使ってユーザー実行モードでSSHログインできる問題があります。ただし、ユーザー実行モードでログインした場合、装置の状態表示は可能ですが、設定操作はできません。

### 2. 当社製品への影響

当社製品の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	本脆弱性に該当しません。
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	
Apresia2000, 3000, 4000, 5000, 13000 シリーズ	AEOS7, AEOS6	
ApresiaNP7000 シリーズ	AEOS-NP7000	本脆弱性に該当します。 対策されたファームウェアをお使いください。 3.回避策を参照
ApresiaNP5000 シリーズ	AEOS-NP5000	
ApresiaNP4000 シリーズ	AEOS-NP4000	
ApresiaNP2000 シリーズ	AEOS-NP2000	
ApresiaLight FM シリーズ	APLFMOS	本脆弱性に該当しません。
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	本脆弱性に該当しません。
HCL Manager Station	
ApresiaManager	
MMRPManager	
Command Navigator	
ApresiaManager/C	
GMXManager	
GMAManager	
BMCManager	
OSWManager	
OAM-LB Navigator	
BFSManager	

### 3. 回避策

対象装置は対策されたファームウェアをお使いください。

機種	対策されたファームウェアとリリース状況
NP7000 シリーズ	AEOS-NP7000 1.04.01 で改修済 (2018年10月)
NP5000 シリーズ	AEOS-NP5000 1.03.07 で改修済 (2018年10月)
NP4000 シリーズ	AEOS-NP4000 1.01.02 で改修済 (2018年11月)
NP2000 シリーズ	AEOS-NP2000 1.04.04 で改修済 (2018年10月)

ファームウェアは以下のサポートサイトからダウンロードしてください。

<https://www.apresia.jp/products/support/index.html>

対策されたファームウェアを適用できない場合、第三者がアクセス可能な環境で SSH サーバー機能を有効にしないでください。

SSH サーバー機能はデフォルトでは無効です。SSH サーバー機能を有効にした後、無効にするには"no ip ssh server"コマンドを用いてください。

第三者が特権実行モードで操作できないように"enable password"を適切に設定してください。

以上