

VLAN 対応ネットワーク機器において、L2 保護機構がバイパスされる問題 (JVNTA#96784241)

1. 脆弱性の概要

細工されたイーサネットフレームにより、VLAN 対応ネットワーク機器におけるデータリンク層 (L2) の種々の保護機構がバイパスされる問題が報告されています。

- ・CVE-2021-27853: VLAN 0 ヘッダと LLC/SNAP ヘッダの組み合わせにより、IPv6 RA Guard や ARP inspection などの保護機構がバイパスされる問題
- ・CVE-2021-27854: VLAN 0 ヘッダと LLC/SNAP ヘッダの組み合わせにより、イーサネットとワイヤレス LAN の間のフレーム変換処理を通じて IPv6 RA Guard などの保護機構がバイパスされる問題
- ・CVE-2021-27861: LLC/SNAP ヘッダを持ち、長さ情報が不正な値になっているフレームにより、IPv6 RA Guard などの保護機構がバイパスされる問題
- ・CVE-2021-27862: LLC/SNAP ヘッダを持ち、長さ情報が不正な値になっているフレームにより、イーサネットからワイヤレス LAN へのフレーム変換処理を通じて IPv6 RA Guard などの保護機構がバイパスされる問題

2. 当社製品への影響

本脆弱性の当社製品への影響有無に関して、以下の表 1~3 に示します。

表 1 ネットワーク装置 1

製品名	OS 名称	影響の有無
Apresia26000 シリーズ	AMIOS6	調査中
Apresia26010QC シリーズ	AMIOS6	
Apresia22000 シリーズ	AMIOS7	
Apresia20000 シリーズ	AMIOS7	
Apresia18000 シリーズ	AMIOS2	
Apresia16000 シリーズ	AMIOS3	
Apresia12000 シリーズ	AMIOS5	
Apresia13000, 15000 シリーズ	AEOS8	非該当
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	
ApresiaNP4000 シリーズ	AEOS-NP4000	
ApresiaNP3000 シリーズ	AEOS-NP3000	
ApresiaNP2500 シリーズ	AEOS-NP2500	
ApresiaNP2100 シリーズ	AEOS-NP2100	
ApresiaNP2000 シリーズ	AEOS-NP2000	
ApresiaLight FM シリーズ	APLFMOS	
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLight GM200 シリーズ	APLGM200OS	
ApresiaLight GS シリーズ	APLGSOS	

表2 ネットワーク装置2

製品名	OS 名称	影響の有無
PONU シリーズ	PONUWare	調査中
APLMC シリーズ	APLMCOS	非該当
XLGMC シリーズ	-	調査中
XGMC シリーズ	-	
GMC シリーズ	-	
BMC シリーズ	-	
ApresiaAERO-5GC-A	-	非該当
ApresiaAERO-CDU100	-	
ApresiaAERO-RU100	-	
ApresiaAERO-UE100	-	
		調査中

表3 ネットワーク管理システム

ソフトウェア名	影響の有無
AP4-GTP-pBroker	非該当
ANRC シリーズ	
HCL Manager Station	
ApresiaManager	
MMRPManager	
Command Navigator	
ApresiaManager/C	
FCRPManager/C	
GMXManager	
GMAManager	
XLGMCManager	
OSWManager	
BMCManager	
OAM-LB Navigator	
BFSManager	

3. 回避策

調査済の装置やシステムにおいて、非該当の場合には不要です。

4. 改訂履歴

2022/11/2 初版

以上