CVE-2021-27861

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-27861
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-27 19:15:00 UTC
Updated	2022-10-12 13:15:00 UTC
Description	Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ieee	ieee 802.2	All	All	All	All
Application	ietf	P802.1q	All	All	All	All

References

Reference	Source	Link
IEEE SA - IEEE/ISO 802.2-1989	CONFIRM	standards.ieee.org
VU#855201 - L2 network security controls can be bypassed using VLAN 0 stacking and/or 802.3 headers	MISC	kb.cert.org
draft-ietf-v6ops-ra-guard-08 - IPv6 Router Advertisement Guard	CONFIRM	datatracker.ietf.org
Layer 2 network security bypass using VLAN 0, LLC/SNAP headers and invalid length | blog.champtar.fr	MISC	blog.champtar.fr
IEEE SA - IEEE P802.1Q	CONFIRM	standards.ieee.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Etienne Champetier (@champtar) <champetier.etienne@gmail.com>

Legacy QID Mappings

317246 Cisco Small Business Switches Bypass Configured First-hop Security (FHS) Vulnerability (cisco-sa-VU855201-J3z8CKTX)

317252 Cisco Catalyst 6500 and 6800 Series Switches Bypass Configured First-hop Security (FHS) Vulnerability (cisco-sa-VU855201-J3z8CKTX)

317253 Cisco Internetwork Operating System (IOS) XR Software Bypass Configured First-hop Security (FHS) Vulnerability (cisco-sa-VU855201-J3z8CKTX)

43997 Arista EOS Multiple Vulnerabilities (SA0080)