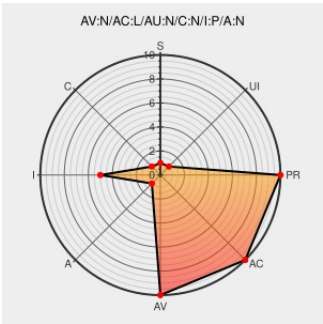
CVE-2005-4441

Published on: 12/20/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4441

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pvlan Protocol from Pvlan Protocol contain the following vulnerability:

The PVLAN protocol allows remote attackers to bypass network segmentation and spoof PVLAN traffic via a PVLAN message with a target MAC address that is set to a gateway router, which causes the packet to be sent to the router, where the source MAC is modified, aka "Modification of the MAC spoofing PVLAN jumping attack," as demonstrated by pvlan.c.

CVE-2005-4441 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051219 Re: Making unidirectional VLAN and PVLAN jumping bidirectional
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051219 Making unidirectional VLAN and PVLAN jumping bidirectional
[Full-disclosure] Making unidirectional VLAN and PVLAN jumping bidirectional	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20051219 Making unidirectional VLAN and PVLAN jumping bidirectional

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pvlan Protocol	Pvlan Protocol	All	All	All	All
Application	Pvlan Protocol	Pvlan Protocol	All	All	All	All

cpe:2.3:a:pvlan_protocol:pvlan_protocol:*:*:*:*:*:*:*:*:

cpe:2.3:a:pvlan_protocol:pvlan_protocol:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→