



CVE-2005-4440

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

Last Modified on: 03/23/2021 11:27:21 PM UTC

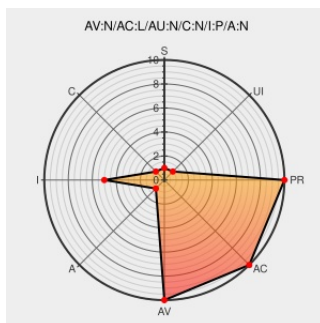
CVE-2005-4440

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Vlan Protocol](#) from [Vlan Protocol](#) contain the following vulnerability:

The 802.1q VLAN protocol allows remote attackers to bypass network segmentation and spoof VLAN traffic via a message with two 802.1q tags, which causes the second tag to be redirected from a downstream switch after the first tag has been stripped, as demonstrated by Yersinia, aka "double-tagging VLAN jumping attack."

CVE-2005-4440 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

SecurityFocus

[www.securityfocus.com](http://www.securityfocus.com/text/html)
[text/html](#)

[BUGTRAQ 20051219 Re: Making unidirectional VLAN and PVLAN jumping bidirectional](#)

SecurityFocus

[www.securityfocus.com](http://www.securityfocus.com/text/html)
[text/html](#)

[BUGTRAQ 20051219 Making unidirectional VLAN and PVLAN jumping bidirectional](#)

[Full-disclosure] Making unidirectional VLAN and PVLAN jumping bidirectional

[web.archive.org](http://web.archive.org/text/html)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[FULLDISC 20051219 Making unidirectional VLAN and PVLAN jumping bidirectional](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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	Vlan Protocol	Vlan Protocol	802.1q	All	All	All
Application	Vlan Protocol	Vlan Protocol	802.1q	All	All	All
cpe:2.3:a:vlan_protocol:vlan_protocol:802.1q:*****:						
cpe:2.3:a:vlan_protocol:vlan_protocol:802.1q:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)