

Cisco Security Response: Making Unidirectional VLAN and PVLAN Jumping Bidirectional

<http://www.cisco.com/warp/public/707/cisco-sr-20051220-pvlan.shtml>

Revision 1.1

Last Updated 2008 June 17 2000 UTC (GMT)

For Public Release 2005 December 20 1800 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is Cisco PSIRT's response to the statements made by Arhont Ltd. in their message: <Making unidirectional VLAN and PVLAN jumping bidirectional>, posted on 2005-Dec-19, to full-disclosure@lists.grok.org.uk. An archived version of the report can be found here:

<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040333.html>

Cisco confirms the statements made.

We would like to thank Arhont Ltd for reporting this issue to us.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

Additional Information

Cisco is aware of VLAN spoofing attacks and recommends that customers apply best practices where possible to reduce the impact of such attacks on their networks. Many best practices are discussed in the document entitled "VLAN Security White Paper", which is available at:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtm

As mentioned in the Arhont advisory, this is a protocol issue with 802.1q VLANs, and not a vendor-specific issue. However, there are techniques available on Cisco devices that may allow you to reduce your exposure to the mentioned attacks.

The document entitled "VLAN Security White Paper" discusses double tagging attacks here:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtm

The publication by Arhont also leverages an IP spoofing component to enable the attack. Cisco recommends IP anti-spoofing techniques and features such as Unicast Reverse Path Forwarding (uRPF) to guard against spoofed IP packets.

The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by IP packets with an spoofed source addresses. It is available on Cisco devices running Cisco IOS and also on Cisco firewalls. For further details on how to configure this feature on IOS devices, please refer to the document entitled "Configuring Unicast Reverse Path Forwarding", which is available at:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_unicast_rpf.html

By enabling Unicast Reverse Path Forwarding (uRPF), all spoofed packets will be dropped at the first device. To enable uRPF, use the following commands.

```
router(config)# ip cef
router(config)# interface FastEthernet0/0
router(config-if)# ip verify unicast reverse-path
```

Revision History

Revision 1.1	2008-June-17	Updated URLs to fix broken links.
Revision 1.0	2005-December-20	Initial public release.

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Send

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)