

[NEWS] Making Unidirectional VLAN and PVLAN Become Bidirectional

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00061.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2005 17:03:54 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Making Unidirectional VLAN and PVLAN Become Bidirectional

SUMMARY

Wepwedgie, a tool by Anton Rager for traffic injection on 802.11 networks protected by WEP, solves the problem of unidirectional communication by bouncing packets from the target host to a third external host under the attackers control. The following article employs the same principle Wepwedgie uses to bypass both VLAN and PVLAN network segmentation.

DETAILS

Vulnerable Systems:

* 802.1q, various PVLAN implementations – This is a protocol, and not vendor-specific attack

1. Modification of the double-tagging VLAN jumping attack:

The attacker tags his malicious data with two 802.1q tags and sends the packet with a spoofed source IP of a host under his or her control. This can be any host to which a valid route from the target VLAN is present, including an external host on the Internet. The first tag gets stripped by the switch the attacker is plugged into and the packet is forwarded to the

[NEWS] Making Unidirectional VLAN and PVLAN Become Bidirectional

next switch. The remaining tag contains a different VLAN number, to which the packet is sent. So, data is forced to pass between the VLANs. The receiving host will check the source IP of the arriving packet and send the reply to this IP, which is a host that belongs to the attacker.

This attack can be launched using

<<http://sourceforge.net/projects/yersinia/>> Yersinia.

2. Modification of the MAC spoofing PVLAN jumping attack:

The attacker sends a packet with a valid source MAC but a spoofed source IP of a host under his or her control. This can be any host to which a valid route from the target PVLAN is present, including an external host on the Internet. The target MAC address is replaced with the one of a gateway router. A switch would forward such packet to the router, which will then look at the IP and direct the packet to the target. Of course, the source MAC of the packet will be replaced by the one of the router, which would then direct the reply packet from the target to the host that belongs to the attacker.

This attack can be launched using `pvlan.c` from the Steve A. Rouiller's "Virtual LAN Security: weaknesses and countermeasures" GIAC Security Essentials Practical Assignment.

Note: Such attacks can be used for different purposes from port scanning to communicating with a backdoor on a different VLAN or PVLAN.

Vendor Status:

While the above advisory is not a vendor specific, Cisco has issued a response:

"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. An archived version of the report can be found here:

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

[NEWS] Making Unidirectional VLAN and PVLAN Become Bidirectional

on their networks. Many best practices are discussed in Cisco's SAFE Blueprint for Layer 2 security:

<[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a0080148701](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a0080148701.html)>
SAFE Layer 2 Security In-depth Version 2

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 Cisco SAFE Blueprint for Layer 2 security discusses double tagging attacks here:

<[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a0080148701](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a0080148701.html)>
VLAN Hopping

The recommended configuration is to disable 802.1q trunking everywhere it is not required so that tagged frames are discarded on ports not configured for trunking.

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 spoofed IP source addresses. It is available on Cisco routers and firewalls. For further details, please refer to:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm>
Configuring Unicast Reverse Path Forwarding

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
router(config-if)# ip verify unicast reverse-path"
```

Disclosure Timeline:
17/10/05 sent to CERT

ADDITIONAL INFORMATION

[NEWS] Making Unidirectional VLAN and PVLAN Become Bidirectional

The information has been provided by <<mailto:mlists@xxxxxxxxxx>> Andrew A. Vladimirov.

The original article can be found at:

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

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [***\[TOOL\] Ciscopack Tool***](#)
 - Next by Date: [***\[NT\] Citrix Program Neighborhood Name Heap Corruption***](#)
 - Previous by thread: [***\[TOOL\] Ciscopack Tool***](#)
 - Next by thread: [***\[NT\] Citrix Program Neighborhood Name Heap Corruption***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)