

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – 802.1q Trunking/VLAN Security</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 1999 September 8</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Cisco Security Procedures</u>	2

Cisco Security Notice: Response to BugTraq – 802.1q Trunking/VLAN Security

Revision 1.0

Last Updated 1999 September 8

Please provide your feedback on this document.

Summary
Details
Cisco Security Procedures

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://www.securityfocus.com/archive/1/26008> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/27062> :

```
To: BugTraq
Subject: Re: VLAN Security
Date: Sep 8 1999 6:59PM
Author: Lisa Napier <lnapier@cisco.com>
Message-ID: <4.2.0.58.19990908175138.00c519c0@twoguys>
In-Reply-To: <37CF858A.FAD4C8F1@orbitel.bg>
```

Hi all,

In our testing, working with default configurations of competitors products, we found roughly the same behavior.

And if you are using ISL, this is not a problem, and packets are dropped accordingly.

The implementation of 802.1q is focused on speed. The changes necessary to function as the Bayswitch does, looking for the 802.1q on input would affect performance. We are discussing the tradeoffs and options with product management at this time.

The use of ISL trunking eliminates this problem, and improperly tagged packets are indeed dropped at the input port. This is due to where this information is located in the frames. ISL tags are prior to the destination mac address, 802.1q tags occur after the destination mac. On

these switches, the input processing only goes as far as the destination mac, and presumes that is all the information needed to make a determination as to where to forward the frame.

It should also be noted that there are configuration workarounds. This can occur ONLY from the native vlan. Forwarding improperly tagged packets across an 802.1q trunk can be avoided by assigning an unused vlan number to the native vlan.

Thank you,

Lisa Napier
Product Security Incident Response Team
Cisco Systems

```
At 11:23 AM 9/3/1999 +0300, Stefan Stefanov wrote:
>bugtraq SIS ALPHAWEST COM AU wrote:
> >
> > To Bugtraq,
> >
> > We have recently conducted some testing into the security of the
> > implementation of VLANs on a pair of Cisco Catalyst 2900 series
> > switches and we feel that the results of this testing might be of some
> > value to the readers. Testing basically involved injecting 802.1q
>> frames with forged VLAN identifiers into the switch in an attempt to
> > get the frame to jump VLANs. A brief background is included below for
> > those that might not be too familiar with VLANs. Others should skip
> > to the end for the results.
> >
> >
> > Interesting proposal, but I think it is more or less Cisco specific.
> > Here I have a BayStack 350T-24 running software revision 1.0.0.2.
> > According to the documentation the switch has the following feature that
> > can be configured on per Port basis:
> >
> > Filter Tagged Frames: Allows you to set this port to filter (discard)
> > all received tagged packets.
> >
> > I think all the ethernet switches should filter all tagged frames when a
> > port is not a trunk port. This way a machine that is connected to a non
> > trunked port, should not be able to send frames with 802.1q tags in it.
> >
> > In your example the switch should have filtered the tagged frames.
> >
> >
--
>Best Regards,
>
>Stefan Stefanov
>Orbitel Ltd.
```

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/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.
