

Cisco Security Response: Cisco VTP Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20070129-vtp.shtml>

Revision 1.2

Last Updated 2007 February 07 1600 UTC (GMT)

For Public Release 2007 January 29 2115 UTC

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

Contents

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

An issue has been reported to the Cisco PSIRT involving malformed VLAN Trunking Protocol (VTP) packets. This attack may cause the target device to reload, causing a Denial of Service (DoS).

Such an attack must be executed on a local ethernet segment, and the VTP domain name must be known to the attacker. Additionally, these attacks must be executed against a switch port that is configured for trunking. Non-trunk access ports are not affected.

This issue is tracked as Cisco Bug ID [CSCsa67294](#) ([registered](#) customers only).

Details

The VLAN Trunking Protocol (VTP) is a Layer 2 protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis in order to maintain VLAN configuration consistency.

VTP packets are exchanged by VLAN-aware switches. For more information on VTP, consult the following link:

http://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_guide_chapter09186a00800e47e3.html.

Upon receiving a malformed VTP packet, certain devices may reload. The attack could be executed repeatedly causing an extended Denial of Service.

In order to successfully exploit this vulnerability, the attacker must know the VTP domain name, as well as send the malformed VTP packet to a port on the switch configured for trunking.

This does not affect switch ports that are configured for voice vlans. A complete Inter-Switch Link (ISL) or 802.1q trunk port is required for the device to be vulnerable.

These platforms are affected:

- Cisco 2900XL Series
- Cisco 2900XL LRE Series

- Cisco 2940 Series
- Cisco 2950 Series
- Cisco 2950-LRE Series
- Cisco 2955 Series
- Cisco 3500XL Series
- Cisco IGESM

No other Cisco products are known to be vulnerable to this issue.

This issue was made public on 26-Jan-2007 on the Full-Disclosure and Bugtraq mailing lists. The Cisco bug ID [CSCsa67294](#) ([registered customers only](#)) was made available to registered customers in May of 2005.

We would like to thank David Barroso Berrueta and Alfredo Andres Omella for reporting this vulnerability to us. You can find their release here: <http://www.s21sec.com/es/avisos/s21sec-034-en.txt>.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities and welcome the opportunity to review and assist in security vulnerability reports against Cisco products.

Workarounds

In order to mitigate your exposure, ensure that only known, trusted devices are connected to ports configured for ISL or 802.1q trunking.

More information on securing L2 networks can be found in the Cisco SAFE Layer 2 Security document at this location: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml

Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.2	2007-February-07	Updated affected platforms list.
Revision 1.1	2007-January-30	Changed 3570 to 3750 in affected platforms list.
Revision 1.0	2007-January-29	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>.

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2006 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).