

Cisco Security Response: Cisco VLAN Trunking Protocol Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20081105-vtp.shtml>

Revision 1.3

Last Updated 2008 November 19 1500 UTC (GMT)

For Public Release 2008 November 5 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Additional Information](#)
[Software Versions and Fixes](#)
[Status of this Notice: FINAL](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the Cisco response to research done by 'showrun.lee' pertaining to a crafted VTP packet denial of service vulnerability.

We would like to thank 'showrun.lee' for reporting this vulnerability to us.

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.

This vulnerability is being addressed by Cisco Bug IDs:

- [CSCsv05934](#) ([registered](#) customers only) —Crafted VTP packet crashes switch running IOS
- [CSCsv54651](#) ([registered](#) customers only) —Crafted VTP packet crashes router with etherswitch module running IOS
- [CSCsv11741](#) ([registered](#) customers only) —Crafted VTP packet crashes switch running CatOS

Cisco PSIRT is aware that exploit code has been made public for this vulnerability.

Additional Information

The VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. When a network administrator makes any configuration changes to the VLAN setup on one device working as a VTP server, said configuration is then distributed via the VTP protocol through all switches in the domain. This reduces the need for replicating this VLAN configuration manually across switches. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst series products using both Cisco IOS and Cisco CatOS system software.

Cisco's VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

Devices without a VTP domain name configured are still vulnerable. For devices not requiring the use of VTP, administrators should set the VTP mode as "transparent" via the CLI command "vtp mode transparent". Devices configured with a VTP domain password are still vulnerable to exploitation, without the malicious attacker knowing the VTP domain password. Switch configuration best practices limit exposure to exploitation, by disabling the Dynamic Trunking Protocol (DTP) on all switch ports that are not required to operate as trunk ports. See [Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software](#) and [Best Practices for Catalyst 4500/4000, 5500/5000, and 6500/6000 Series Switches Running CatOS Configuration and Management](#) for further information.

Products affected by this vulnerability:

- Devices running affected versions of Cisco IOS or CatOS that have VTP Operating Mode as either "server" or "client".
- Devices running affected versions of Cisco IOS with Ethernet Switch Modules for Cisco 1800/2600/2800/3600/3700/3800 Series Routers that have VTP Operating Mode as either "server" or "client".

Products not affected by this vulnerability:

- Devices configured with VTP operating mode as "transparent".
- Devices configured with VTP version 3 (CatOS only)
- Devices configured with VTP operating mode as "off" (CatOS only)

To determine the current VTP operating mode on a Cisco device, log into the device and issue the **show vtp status** command on an IOS device or the **show vtp domain** command on a CatOS device. Switches that show either "server" or "client" as the VTP operating mode are affected by this vulnerability.

The following example shows a device running Cisco IOS and operating in VTP "server" mode:

```
ios_switch#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode       : Server
VTP Domain Name            : test
VTP Pruning Mode           : Disabled
```

```

VTP V2 Mode                : Enabled
VTP Traps Generation       : Disabled
MD5 digest                  : <removed>
Configuration last modified by 0.0.0.0 at 3-1-93 04:02:09
ios_switch#

```

The following example shows a device running Cisco CatOS and operating in VTP "server" mode:

```

catos_switch> (enable) show vtp domain
Version      : running VTP1 (VTP3 capable)
Domain Name  : test                Password : not configured
Notifications: disabled          Updater ID: 0.0.0.0

Feature      Mode          Revision
-----
VLAN         Server       2

Pruning      : disabled
VLANs prune eligible: 2-1000
catos_switch> (enable)

```

Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Cisco is currently patching these Cisco bug IDs into Cisco IOS and Cisco CatOS software. To check on the latest versions with fixed releases please consult the Cisco Bug Toolkit <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs> or click on the Cisco Bug IDs within the Cisco Response section of this response.

Status of this Notice: FINAL

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.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Revision History

Revision 1.3	2008- November-19	Added Software Versions and Fixes section.
Revision	2008-	

1.2	November-7	Added bug ID CSCsv54651
Revision 1.1	2008-November-6	Updated products not affected
Revision 1.0	2008-November-5	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.](#)