

# Cisco Security Response: Cisco VLAN Trunking Protocol Vulnerabilities

Document ID: 71306

<http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

## Revision 1.0

For Public Release 2006 September 13 1700 UTC (GMT)

---

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

---

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

---

## Cisco Response

This is a Cisco response to an advisory published by FX of Phenoelit posted as of September 13, 2006, at <http://www.securityfocus.com/archive/1/445896/30/0/threaded>, and entitled "Cisco Systems IOS VTP multiple vulnerabilities".

We would like to thank FX and Phenoelit Group for reporting these vulnerabilities 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.

These vulnerabilities are addressed by Cisco Bug IDs:

- [CSCsd52629](#) ([registered](#) customers only), [CSCsd34759](#) ([registered](#) customers only) VTP version field DoS
- [CSCse40078](#) ([registered](#) customers only), [CSCse47765](#) ([registered](#) customers only) Integer Wrap in VTP revision
- [CSCsd34855](#) ([registered](#) customers only), [CSCei54611](#) ([registered](#) customers only) Buffer Overflow in VTP VLAN name
- [CSCsg03449](#) ([registered](#) customers only) Etherswitch module VLAN Trunking Protocol Vulnerabilities

## Additional Information

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 you configure a new VLAN on one VTP server, the VLAN configuration information is distributed via the VTP protocol through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst series products in both Cisco IOS and Cisco CatOS system software.

Products affected by these vulnerabilities:

- Switches running affected versions of Cisco IOS<sup>®</sup> software that have VTP Operating Mode as either "server" or "client" are affected by all three vulnerabilities.
- Switches running affected versions of Cisco CatOS that have VTP Operating Mode as either "server" or "client" are only affected by the "Integer Wrap in VTP revision" vulnerability.
- Ethernet Switch Modules for Cisco 1800/2600/2800/3600/3700/3800 Series Routers that have VTP Operating Mode as either "server" or "client" are affected by all three vulnerabilities.

Products not affected by these vulnerabilities:

- Switches configured with VTP operating mode as "transparent"
- Switches running CatOS with VTP Operating Mode as either "server" or "client" are not affected by the "Buffer Overflow in VTP VLAN name" or "VTP Version field DoS" vulnerabilities

To determine the VTP mode on the switch, log in to 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 these vulnerabilities.

An example is shown below for Cisco IOS software with VTP operating in "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#
```

An example is shown below for Cisco CatOS with VTP operating in "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)
```

- **VTP Version field DoS**

The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition. When a switch receives a specially crafted summary packet, the switch will reset with a Software Forced Crash Exception. Messages for either "watchdog timeout" or "CPU hog" for process VLAN Manager will be seen prior to the software reset within the syslog messages generated by the switch. The packets must be received on a trunk enabled port.

Switches running CatOS are not affected by this vulnerability and will display a log message

```
"%VTP-2-RXINVSUMMARY:rx invalid summary from [port number]"
```

should a specially crafted summary packet be received.

There are no workarounds for this vulnerability.

Switches configured with a VTP domain password are still affected by this vulnerability.

Cisco recommends that customers upgrade to a version of Cisco IOS software that contains the fixes for either [CSCsd52629](#) ([registered](#) customers only) or [CSCsd34759](#) ([registered](#) customers only) .

- **Buffer Overflow in VTP VLAN name**

The VTP feature in certain versions of Cisco IOS software is vulnerable to a buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error. The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

Applying a VTP domain password to the VTP domain will prevent spoofed VTP summary advertisement message from advertising an incorrect VLAN name. Refer to

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking\\_solutions\\_white\\_paper09186a0080](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a0080) for further information on setting VTP domain passwords.

- **Integer Wrap in VTP revision**

The VTP feature in certain versions of Cisco IOS software and Cisco CatOS software will display statistic counters as a negative number due to an integer wrap. Normal VTP operation will occur if no changes are made within the VTP domain. With addition of switches or resetting of a VTP server configuration revision, potentially VTP updates may not be processed by other VTP servers/clients within the domain. Should the switches be impacted by this vulnerability, customers should execute the recovery procedures as listed below. Once the VTP configuration revision exceeds 0x7FFFFFFF, the output for the VTP configuration revision in **show vtp status** (on an IOS device) or **show vtp domain** (on a CatOS device) will display as a negative number. Operation of the switch is not affected, however further changes to the VLAN database may not be properly propagated throughout the VTP domain.

Any crafted VTP packet with a change in the configuration revision must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

Example from Cisco IOS:

```
ios_switch#show vtp status
VTP Version                : 2
Configuration Revision      : -2147483648
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 17
VTP Operating Mode         : Client
VTP Domain Name            : psirt
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : <removed>
Configuration last modified by 0.0.0.0 at 3-1-93 00:10:07
ios_switch#
```

Example from Cisco CatOS:

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

Feature      Mode      Revision
-----
VLAN         Server   -2147483648

Pruning      : disabled
VLANs prune eligible: 2-1000
```

Applying a VTP domain password to the VTP domain will prevent spoofed VTP summary advertisement messages from advertising 0x7FFFFFFF as a configuration revision number. Refer to [http://www.cisco.com/en/US/products/hw/switches/ps646/products\\_configuration\\_guide\\_chapter09186a00801](http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a00801) for further information on setting VTP domain passwords.

To recover from the negative configuration revision due to exploitation, the following methods can be performed to recover the VTP domain operations:

- Change VTP domain names on all switches.
- Change all VTP servers/clients to transparent mode first. Then change back to their original server/client mode.

For further information on VTP, please refer to

[http://www.cisco.com/en/US/tech/tk389/tk689/technologies\\_tech\\_note09186a0080094c52.shtml](http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml).

For further information on Layer 2 security practices, please refer to

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking\\_solutions\\_white\\_paper09186a008014870f](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f).

## Revision History

Revision 1.0	2006 – September – 13	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](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>.

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Sep 13, 2006

Document ID: 71306

---