

# Table of Contents

- Cisco Security Notice: Response to BugTraq – Cisco VPN 3000 Gateway MTU Overflow.....1**
- Revision 1.0.....1
- Last Updated 2002 July 15.....1
- Please provide your feedback on this document.....1
- Summary.....1
- Details.....1
- Cisco Security Procedures.....3

# Cisco Security Notice: Response to BugTraq – Cisco VPN 3000 Gateway MTU Overflow

## Revision 1.0

Last Updated 2002 July 15

---

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/1/281544> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/282316> .

To: BugTraq  
Subject: Re: Cisco VPN3000 gateway MTU overflow  
Date: Jul 15 2002 3:31PM  
Author: Pete Davis <psd@cisco.com>  
Message-ID: <OAENJKOBHBMFELMPDAILEEPPCOAA.psd@cisco.com>

Thanks for the comments on problems you are experiencing. I did not receive a response to any of the previous messages I sent you, so I have copied the Bugtraq list, in case you do not receive email sent to your reply to address.

In general, the best way to report product problems is to open up a case with the Cisco TAC (Tech Support) and our TAC will work with you to go through your issues and help find a resolution. If you open a TAC case in the future and you aren't satisfied, you should feel free to ask for the case to be escalated. Any problems that are found will have bug IDs assigned to them so that we can track and fix them for you as soon as possible. All open bugs are visible by all customers in our Bug Tracker tool on [cco.cisco.com](http://cco.cisco.com).

Security related items are handled through our PSIRT group ([psirt@cisco.com](mailto:psirt@cisco.com)), which helps coordinate getting a fix and response out as soon as possible including distribution of information to Bugtraq and various other mailing lists.

Since your issue report appears at first glance to be problem related, I

will do my best to help respond. If you have specific questions or additional information, please feel free to drop it to me directly and we will work to help you resolve problems you are experiencing. If you a specific support case #, please attach this in your email to me as well. This information will help to make sure that we have all the details on your specific environment so that if you have found a new problem, we can ensure it is corrected ASAP.

Our next release will offer some additional nice enhancements regarding fragmentation, Path MTU Discovery (PMTUD) and Client MTU determination.

Specifically-

1. Ability to choose whether or not large packet fragmentation is performed before or after encapsulation "pre-fragmentation" as well as whether or not the Concentrator responds to internal ICMP/PMTUD requests and requests an internal device to lower its MTU, or otherwise fragments the packet and clears the DF bit if set. The main reason that this will be a configurable option is due to the fact that specific service packets of Windows 2000 and some other OS's do not respond to PMTUD when the request comes from a client on the same subnet as the server. (Concentrator)
2. Ability to define a maximum Concentrator MTU < default of ~15XX bytes (Concentrator)
3. Adjusted setMTU behavior to fix specific NDISWAN/dial-up related issues that may presently require manual MTU adjustment workaround (Client)

The setMTU application is needed on the client side regardless of anything on the Concentrator side. In most cases (and we strive for all), running it manually should be unnecessary. There are some enhancements with our next release that fix a couple of specific dial-up/NDISWAN issues on the client side.

If you are interested in specifically trying out our new release and providing beta feedback as to whether or not your problem is resolved or would like us to help to resolve your issues, you can feel free to contact me directly. Since the concentrator does fragment large packets, it would be interesting to know if you're seeing 1580 byte packets on the wire or the 1580 byte packet fragmented based on the Ethernet MTU of 1518. In order to investigate and resolve the problems you are reporting, please send me information concerning your application/environment, MTU on the Client, Concentrator configuration, device on the public side of the Concentrator exhibiting problems and a sniffer trace showing 1580 byte packets on the wire or other problems you are seeing.

I look forward to hearing back from you so that we can help resolve your problems.

Best Regards,  
-Pete Davis  
Cisco Systems, Inc.  
(508) 553-6007

<ATTACHMENT>

Cisco VPN3000 gateway MTU overflow =====

Bug class: Conceptual/bad protocol implementation  
Equipments affected: Cisco/VPN 3000 Concentrator with  
software vpn3000-3.5.Rel-k9.bin

FACTS

The Cisco VPN3000 gateway lets remote client dictate which maximum MTU to use when sending back ESP frames, regardless of the transmitting capabilities of the physical medium.

#### IMPACT

- \* Oversized frames get silently discarded by equipments linked to the gateway's public interface and retransmissions occur.
- \* Other disturbances or DoS against neighboring equipments may occur, especially as many IP stacks on routers and sniffers etc ... are poorly implemented.

#### DETAILS

We have witnessed this phenomena after establishing tunnels with the "VPN dialer" over a modem connexion: when the target sends back ethernet frames with size close to the max ethernet MTU (1500), the gateway encrypts the frames adding ESP headers and stupidly tries to send a 1580-bytes frame back to the client.

#### RESOLUTION

-> From the official documentation there is no way to enforce a maximum MTU on the VPN gateway.  
-> Hence: a gateway software patch by Cisco is necessary: if MTU negotiation occurs, the gateway should set a max-MTU threshold (the physical medium's !).

#### PSEUDO WORKAROUNDS

\* client side: For Windows-based OS (likely Unix and Linux-based OS too), Cisco released a tool called setMTU.exe that can prevent ill MTU negotiation from happening.

\* target side: artificially lowering the max MTU on the interfaces.

-> But such a policy is not acceptable:  
The VPN client, as well as remote targets, should not have to be aware of the gateway's interface configuration !

The bug does not lie in client software, but in the gateway's software.

Master Phi

</ATTACHMENT>

## 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](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>.

---

