

Cisco Security Advisory: VPN 3000 Concentrator IP Options

Document ID: 13646

Advisory ID: cisco-sa-20010412-vpn3kipoptions

<http://www.cisco.com/warp/public/707/cisco-sa-20010412-vpn3kipoptions.shtml>

Revision 1.0

For Public Release 2001 April 12 1500 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Workarounds
Obtaining Fixed Software
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Summary

If a crafted IP packet, with an invalid IP Option setting is transmitted to a VPN 3000 series concentrator on the same network segment (no routers in between), it can cause the VPN 3000 series concentrator to hang with a 100% CPU Utilization. The concentrator would then have to be reset. After rebooting, the equipment would function normally until the crafted IP packet is received again. The defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability is described in Cisco bug id CSCds92460.

This notice will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20010412-vpn3kipoptions.shtml>

Affected Products

This section provides details on affected products.

Vulnerable Products

Cisco VPN 3000 series concentrators running software releases up to but not including revision 2.5.2 (F) are affected by this vulnerability. This series includes models 3005, 3015, 3030, 3060, and 3080.

To determine if a Cisco VPN 3000 series concentrator is running affected software, check the revision via the web interface or the console menu.

Products Confirmed Not Vulnerable

Any VPN 3000 series concentrators running revision 2.5.2 (F) or later are unaffected by this vulnerability.

This vulnerability does not affect the VPN 5000 series concentrators. No other Cisco product is known to be affected by this vulnerability.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

If a crafted IP packet, with an invalid IP Option setting, is transmitted to a VPN 3000 series concentrator on the same network segment (no routers in between), on either the Inside or the Outside interface, it can cause the VPN 3000 series concentrator to hang with a 100 % CPU Utilization. The concentrator would then have to be reset via the console port as no SNMP or HTTP remote management control would be possible. After rebooting, the equipment would function normally until the crafted IP packet is received again.

In order to exploit this vulnerability the attacker must be on the same network segment as the concentrator without any routers in between. A crafted IP packet traversing a router would typically get its invalid IP Options dropped and would not be able to affect the VPN 3000 series concentrator.

The vulnerability is documented as Cisco bug id CSCds92460.

Impact

When this crafted IP packet is received by the VPN 3000 series concentrator, the concentrator will stop passing traffic and will not respond to any management inquiries via SNMP, Telnet or HTTP. However management via the console port is possible.

For VPN 3000 series concentrator models 3015, 3030, 3060, and 3080 the CPU Utilization bar graph indicator on the front panel will go to 100%.

Software Versions and Fixes

The vulnerability has been fixed in revision 2.5.2 (E) code. The fix will be carried forward into all future releases.

However due to the advisory at <http://www.cisco.com/warp/public/707/vpn3k-telnet-vuln-pub.shtml> the recommended revision to upgrade to is 2.5.2 (F)

Upgrade can be done via the remote software upgrade feature using the VPN 3000 series concentrator's web based management interface.

Workarounds

There are no system configuration workarounds. Please upgrade to revision 2.5.2 (F) code.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

This was reported to Cisco by a customer who accidentally discovered this vulnerability.

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.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20010412-vpn3kipoptions.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 1.0	2001-April-12	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>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Apr 12, 2001

Document ID: 13646
