

Cisco Security Advisory: Cisco IOS Software Network Time Protocol Packet Vulnerability

Advisory ID: cisco-sa-20090923-ntp

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml>

Revision 1.0

For Public Release 2009 September 23 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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

Cisco IOS® Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml>.

Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

Cisco IOS Software devices are vulnerable if they support NTPv4 and are configured for NTP operations. NTP is not enabled in Cisco IOS Software by default.

To see if a device supports NTPv4, log into the device and via configuration mode of the command line interface (CLI), enter the command **ntp peer 127.0.0.1 version ?**. If the output has the number **4** as an option, then the device supports NTPv4. The following example identifies a Cisco device that is running a Cisco IOS Software release that does support NTPv4:

```
Router#configure terminal
Router(config)#ntp peer 127.0.0.1 version ?
<2-4> NTP version number
```

The following example identifies a Cisco device that is running a Cisco IOS Software release that does not support NTPv4:

```
Router(config)#ntp peer 127.0.0.1 version ?  
<1-3> NTP version number
```

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>  
ntp peer <any following commands>  
ntp server <any following commands>  
ntp broadcast client  
ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
router#show running-config | include ntp  
ntp peer 192.168.0.12
```

The following example identifies a Cisco device that is not configured with NTP:

```
router#show running-config | include ntp  
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version  
Cisco Internetwork Operating System Software  
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3  
(26), RELEASE SOFTWARE (fc2)
```

Technical Support: <http://www.cisco.com/techsupport>
Copyright ©) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-
ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ©) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

<output truncated>

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link: <http://www.cisco.com/warp/public/620/1.html>.

☐ Products Confirmed Not Vulnerable


The following products and features are not affected by this vulnerability:


- Cisco IOS Software devices without support for NTPv4
- Cisco IOS Software devices configured with only Simple NTP (SNTP) feature
- Cisco IOS XE Software
- Cisco IOS XR Software

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs over UDP, which in turn runs over IP. NTPv3 is documented in [RFC1305](#) .

NTPv4 is a significant revision of the NTP standard, and is the current development version, but has not been formalized into an RFC at the time of publication of this advisory. NTPv4 is currently documented in [draft-ietf-ntp-ntp4-01](https://www.ietf.org/archive/id/draft-ietf-ntp-ntp4-01.html) 

When a Cisco IOS Software device supporting NTPv4 receives a specific NTP packet it will crash while creating the NTP reply packet. The NTP packet can be sent from any remote device, and does not require authentication. Cisco IOS devices supporting NTPv4 and configured with NTP peer authentication are still vulnerable. The device does not have to be explicitly configured for NTPv4 peers. For example a device configured with all NTP peers being explicitly labeled as version 2 would still be vulnerable, as shown in the following example:

```
Router#show running-config | include ntp
ntp peer 192.168.0.254 version 2
ntp peer 192.168.0.1 version 2
Router#
```

For further information on the Cisco implementation of NTP, consult the configuration guide "Cisco IOS and NX-OS Software - Performing Basic System Management" at the following link: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1001170

This vulnerability is documented in the following Cisco Bug IDs: [CSCsu24505](#) ([registered customers only](#)) and [CSCsv75948](#) ([registered customers only](#)) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-2869. Both Cisco bug IDs are required for a full fix to this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsu24505/CSCsv75948: Cisco IOS Software NTP Packet Vulnerability					
Calculate the environmental score of CSCsu24505 and CSCsv75948					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

[-] Impact

Successful exploitation of the vulnerability may result in a reload of the device. The vulnerability could be repeatedly exploited to cause an extended DoS condition.

[Top of the section](#) [Close Section](#)

[-] 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.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases		
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.2 based releases		
Affected 12.3-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.3 based releases		

Affected 12.4-Based Releases	First Fixed Release	Recommended Release
12.4	Not Vulnerable	
12.4GC	Not Vulnerable	
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Releases prior to 12.4(22)MD are not vulnerable, vulnerability was first introduced in 12.4(22)MD, first fixed in 12.4(22)MD1.	12.4(22)MD1

12.4MDA	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	<p>Releases prior to 12.4(20)T are not vulnerable.</p> <p>12.4(20)T and 12.4(20)T1 are vulnerable, vulnerability is first fixed in 12.4(20)T2.</p> <p>12.4(22)T is vulnerable, vulnerability is first fixed in 12.4(22)T1</p> <p>12.4(24)T is not vulnerable.</p>	<p>12.4(20)T4</p> <p>12.4(22)T3</p> <p>12.4(24)T2; Available on 23-OCT-2009</p>
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	
12.4XD	Not Vulnerable	
12.4XE	Not Vulnerable	

12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	

12.4XZ	Vulnerable; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YA	Vulnerable; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YB	Not Vulnerable	
12.4YD	12.4(22)YD1	12.4(22)YD1
12.4YE	12.4(22)YE1	12.4(22)YE1

[Top of the section](#) [Close Section](#)

Workarounds

There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note: NTP peer authentication is **not** a workaround and is still a vulnerable configuration.

NTP Access Group



Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast

RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access
```

```
access-list 1 permit 171.70.173.55
```

```
!--- Apply ACE to the NTP configuration
```

```
ntp access-group peer 1
```



Warning: Depending on your NTP ACL configuration, be aware of Cisco Bug ID: [CSCsw79186](#) ([registered](#) customers only) - NTPv4 server treats NTPv3 client as a 'peer'.

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

Infrastructure Access Control Lists



Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
```

```
!--- Feature: Network Time Protocol (NTP)
```

```
!---
```

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES
WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
```

!--- Note: If the router is acting as a NTP broadcast client

!--- via the interface command "ntp broadcast client"
!--- then broadcast and directed broadcasts must be
!--- filtered as well. The following example covers
!--- an infrastructure address space of 192.168.0.X

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES
WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES
WILDCARD
    host 255.255.255.255 eq ntp
```

!--- Note: If the router is acting as a NTP multicast client

!--- via the interface command "ntp multicast client"
!--- then multicast IP packets to the mutlicast group
must
!--- be filtered as well. The following example covers
!--- a NTP multicast group of 239.0.0.1 (Default is
!--- 224.0.1.1)

```
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES
WILDCARD
    host 239.0.0.1 eq ntp
```

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

```
access-list 150 deny udp any
```

```
!--- Permit/deny all other Layer 3 and Layer 4 traffic in  
!--- accordance with existing security policies and  
!--- configurations. Permit all other traffic to transit  
the  
!--- device.
```

```
access-list 150 permit ip any any
```

```
!--- Apply access-list to all interfaces (only one example  
!--- shown)
```

```
interface fastEthernet 2/0  
ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Control Plane Policing

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)
```

```
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 123
```

```
!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.
```

```
access-list 150 permit udp any any eq 123
```

```
!--- Permit (Police or Drop)/Deny (Allow) all other
Layer3 and
!--- Layer4 traffic in accordance with existing security
policies
!--- and configurations for traffic that is authorized to
be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
```

```
class-map match-all drop-udp-class
    match access-group 150
```

```
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
```

```
policy-map drop-udp-traffic
    class drop-udp-class
        drop
```

```
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
```

```
control-plane
    service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS Software trains:

```
policy-map drop-udp-traffic
class drop-udp-class
police 32000 1500 1500 conform-action drop exceed-action
drop
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, "Control Plane Policing Implementation Best Practices" and "Cisco IOS Software Releases 12.2 S - Control Plane Policing" at the following links: http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

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

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

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

This vulnerability was discovered by Cisco when handling customer support calls.

☐ **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 is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.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
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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	2009-September-23	Initial public release
--------------	-------------------	------------------------

[Top of the section](#) [Close Section](#)

☐ 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>.

[Top of the section](#) [Close Section](#)

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)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)