

Cisco Security Advisory: NTP Vulnerability

Advisory ID: cisco-sa-20020508-ntp-vulnerability

<http://www.cisco.com/warp/public/707/cisco-sa-20020508-ntp-vulnerability.shtml>

Revision 2.1

Last Updated 2003 October 02 0200 UTC (GMT)

For Public Release 2002 May 08 1600 UTC (GMT)

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

Contents

[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

Network Time Protocol (NTP) is used to synchronize time on multiple devices. A vulnerability has been discovered in the NTP daemon query processing functionality. This vulnerability has been publicly announced.

The following products are identified as affected by this vulnerability:

- All releases of Cisco IOS software
- Media Gateway Controller (MGC) and related products
- BTS 10200
- Cisco IP Manager

Other Cisco software applications may run on Solaris platforms and where those products have not specifically been

identified, customers should install security patches regularly in accordance with their normal maintenance procedures.

Cisco is continuing to research this issue in other products that may be affected. Unless explicitly stated otherwise, all other products are considered to be unaffected.

There are [workarounds](#) available to mitigate the effects.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20020508-ntp-vulnerability.shtml>.

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

☐ **Affected Products**

This section provides details on affected products.

☐ **Vulnerable Products**

The following products are affected:

- All releases of Cisco IOS software
- Media Gateway Controller (MGC) and related products, they encompass the following products:
 - SC2200
 - Cisco Virtual Switch Controller (VSC3000)
 - Cisco PGW2200 Public Switched Telephone Network (PSTN) Gateway
 - Cisco Billing and Management Server (BAMS)
 - Cisco Voice Services Provisioning Tool (VSPT)
- BTS 10200
- Cisco IP Manager

Other Cisco software applications may run on Solaris platforms and where those products have not specifically been identified, customers should install security patches regularly in accordance with their normal maintenance procedures.

☐ **Products Confirmed Not Vulnerable**

The following products are *not* affected:

- Cisco routers 1600/1600-R, running an IP-only image
- Cisco routers 801, 803, 811, 813, 1003
- Cisco Content Service Switch 11000 Series
- Cisco Secure PIX Firewall
- Catalyst 6000 family switches, all CatOS releases
- Catalyst 5000 family switches, all CatOS releases
- Catalyst 4000 family switches, all CatOS releases

Cisco is continuing to research this issue in other products that may be affected. Unless explicitly stated otherwise, all other products are considered to be not affected.

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


☐ **Details**

By sending a crafted NTP control packet, it is possible to trigger a buffer overflow in the NTP daemon. This

vulnerability can be exploited remotely. The successful exploitation may cause arbitrary code to be executed on the target machine. Such exploitation, if it is possible at all, would require significant engineering skill and a thorough knowledge of the internal operation of Cisco IOS software or SUN Solaris operating system.

The vulnerability is present regardless of the role played by the device. The device may be an NTP server or client and it will still be vulnerable.

For IOS, this vulnerability is documented as Cisco Bug ID **CSCdt93866** and **CSCdw35704**.

The main repository of NTP software and all other information regarding NTP, can be found at <http://www.ntp.org/> .


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

☐ Impact

The successful exploitation may cause arbitrary code to be executed on the target machine. More often, an attempt to exploit this vulnerability will result in a daemon or device crash.

- **Cisco IOS**

An IOS running device is vulnerable to a malformed ntp control packet. This may be exploited to cause the router to crash. Repeated exploitation of this vulnerability may result in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.

This vulnerability has been publicly announced on the Bugtraq mailing list (for the original report see <http://www.securityfocus.com/archive/1/175701> ).

- **MGC and Related Products**

- **Cisco IP Manager**

- **BTS 10200**

The xntpd daemon that is used as a part of the Solaris installation is vulnerable.

By exploiting this vulnerability it is only possible to crash the xntpd itself. According to the available information, it seems that it is not possible to execute the arbitrary code.

[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.

MGC and Related Products

MGC and related products are running on three different Solaris versions.

- Solaris 2.5.1

The patch has not been released by Sun.

- Solaris 2.6

For the software running on Solaris 2.6, the patch is available within the CSCOh007.pkg package. This

package can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-sol> but you must be a registered user and be logged in.

- Solaris 2.8

For the software running on Solaris 8, the patch is available within the MGCSOL8-h015 package. This package can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-sol8> but you must be a registered user and be logged in.

Cisco IP Manager

BTS 10200

The customers should install the latest Recommended Solaris Patch Cluster available from <http://sunsolve.Sun.COM/pub-cgi/show.pl?target=patches/patch-access>. 

Cisco IOS

Each row of the following table describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix and the anticipated date of availability for each are listed in the Rebuild, Interim, and Maintenance columns. A device running any release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep the following definitions in mind:

- **Maintenance**
Most heavily tested and highly recommended release of any label in a given row of the table.
- **Rebuild**
Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to affect the repair.
- **Interim**
Built at regular intervals between maintenance releases and receives less testing. Interim releases should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available via manufacturing, and usually are not available for customer download from CCO without prior arrangement with the Cisco TAC.

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 TAC for assistance as shown in the [Obtaining Fixed Software](#) section.

More information on IOS release names and abbreviations is available at <http://www.cisco.com/web/about/security/intelligence/ios-ref.html>.

Train	Image or Platform Description	Availability of Fixed Releases*		
11.0-based Releases and Earlier	Rebuild	Interim**	Maintenance	

10.3	Multiple releases and platforms	End of Engineering
		Upgrade recommended
11.0	Multiple releases and platforms	End of Engineering
		Upgrade recommended to 12.0(23)
11.1	Major release for all platforms	End of Engineering
		Upgrade recommended to 12.0(23)
11.1AA		End of Engineering
		Upgrade recommended to 12.1(16)
11.1CA		End of Engineering
		Upgrade recommended
11.1CC		End of Engineering
		Upgrade recommended
11.1CT		End of Engineering
		Upgrade recommended to 12.0ST
11.1IA		End of Engineering
		Upgrade recommended to 12.2(10)

11.2	Major release for all platforms	End of Engineering
		Upgrade recommended to 12.0(23)
11.2BC		End of Engineering
		Upgrade recommended to 12.1(16)
11.2F		End of Engineering
		Upgrade recommended to 12.0(23)
11.2GS		End of Engineering
		Upgrade recommended to 12.0(23)
11.2P		End of Engineering
		Upgrade recommended to 12.0(23)
11.2SA		End of Engineering
		Upgrade recommended to 12.0W
11.2WA4		End of Engineering
		Upgrade recommended to 12.0W
11.2XA		End of Engineering
		Upgrade recommended to 12.0(23)

11.3-based Releases		Rebuild	Interim**	Maintenance
11.3	Major release for all platforms	End of Engineering		
		Upgrade recommended to 12.0(23)		
11.3AA	ED for dial platforms and access servers: 5800, 5200, 5300, 7200	Not Scheduled		
		Upgrade recommended to 12.1(16)		
11.3DA	Early deployment train for ISP DSLAM 6200 platform	End of Engineering		
		Upgrade recommended to 12.3		
11.3DB	Early deployment train for ISP/Telco/PTT xDSL broadband concentrator platform, (NRP) for 6400	End of Engineering		
		Upgrade recommended to 12.2B		
11.3HA	Short-lived ED release for ISR 3300 (SONET/SDH router)	End of Engineering		
		Upgrade recommended to 12.0(23)		
11.3MA	MC3810 functionality only	End of Engineering		
		Upgrade recommended to 12.1(16)		
11.3NA	Voice over IP, media convergence, various platforms	End of Engineering (16)		
		Upgrade recommended to 12.1		

11.3T	Early deployment major release, feature-rich for early adopters	End of Engineering		
		Upgrade recommended to 12.0(23)		
11.3XA	Introduction of uBR7246 and 2600	End of Engineering		
		Upgrade recommended to 12.0(23)		
11.3WA4	LightStream 1010	End of Engineering		
		Upgrade recommended to 12.0WA		
12.0-based Releases		Rebuild	Interim**	Maintenance
12.0	General Deployment release for all platforms		12.0(22.4)	12.0(23)
12.0DA	xDSL support: 6100, 6200	Not Scheduled		
		Upgrade recommended to 12.2T		
12.0DB	Early Deployment (ED) release, which delivers support for the Cisco 6400 Universal Access Concentrator (UAC) for Node Switch Processor (NSP).	Not Scheduled		
		Upgrade recommended to 12.2B		
	Early Deployment (ED) release, which delivers support for the Cisco	Not Scheduled		

12.0DC	6400 Universal Access Concentrator (UAC) for Node Switch Processor (NSP).	Upgrade recommended to 12.2B		
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(16)S9, 12.0(21)S3	12.0(21.4)S, 12.0(22.3)S1	12.0(22)S
12.0SC	Cable/broadband ISP: uBR7200	Not Scheduled		
		Upgrade recommended to 12.1(13)EC1		
12.0SL	10000 ESR: c10k	Not Scheduled		
		Upgrade recommended to 12.0(23)S3		
12.0SP	Early deployment release	12.0(21)SP1		
12.0ST	Cisco IOS software Release 12.0ST is an early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000 (GSR) series routers for Service Providers (ISPs).	12.0(21)ST3		
12.0SY	Early deployment release	12.0(21.4)SY		12.0(22)SY
12.0T	Early Deployment(ED): VPN, Distributed Director, various platforms	Not Scheduled		
		Upgrade recommended to 12.1(16)		

12.0W	Catalyst switches: cat8510c, cat8540c, c6msm, ls1010, cat8510m, cat8540m			12.0(24)W5(26)
12.0W	Catalyst switches: cat2948g, cat4232			12.0(25)W5(27)
12.0W	Catalyst switches: cat5000ATM			12.0(24)W5(26a)
12.0WC		12.0(5)WC5a		
12.0WT	cat4840g	Not Scheduled		
		Upgrade to be determined		
12.0XA	Early Deployment (ED): limited platforms	Not Scheduled		
		Upgrade recommended to 12.1(16)		
12.0XB	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.1(16)		
12.0XC	Early Deployment (ED): limited platforms	Not Scheduled		
		Upgrade recommended to 12.1(16)		
	Early	Not Scheduled		

12.0XD	Deployment (ED): limited platforms	Upgrade recommended to 12.1(16)
12.0XE	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(8b)E14
12.0XF	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0XG	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0XH	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0XI	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0XJ	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0(5)XK	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0(7)XK	Early Deployment	Not Scheduled

	(ED): limited platforms	Upgrade recommended to 12.2(10)
12.0XL	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0XM	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(8)T
12.0XN	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0XP	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.0(5)WC5a
12.0XQ	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.1(16)
12.0XR	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(10)
12.0XS	Early Deployment (ED): limited platforms	End of Engineering
		Upgrade recommended to 12.1(8b)E14
12.0XU	Early Deployment (ED): limited	Not Scheduled

	platforms	Upgrade recommended to 12.0(05)WC05a		
12.0XV	Early Deployment (ED): limited platforms	Not Scheduled		
		Upgrade recommended to 12.2(10)		
12.1-based Releases		Rebuild	Interim**	Maintenance
12.1	General deployment release for all platforms		12.1(15.3)	12.1(16)
12.1AA	Dial support	Not Scheduled		
		Upgrade recommended to 12.2(10)		
12.1DA	xDSL support: 6100, 6200	Not Scheduled		
		Upgrade recommended to 12.2T		
12.1DB	Cisco IOS Software Release 12.1(1)DB supports the Cisco 6400 Universal Access Concentrator			12.2(15)B
12.1DC	Cisco IOS Software Release 12.1(1)DC supports the Cisco 6400 Universal Access Concentrator			12.2(15)B
12.1E	Enterprise	12.1(8b)E14, 12.1(12c)E1	12.1(12.5)E, 12.1(18.1)E	12.1(19)E

12.1EA	Catalyst 3550			12.1(11)EA1
12.1EC	12.1EC is being offered to allow early support of new features on the uBR7200 platform, as well as future support for new Universal Broadband Router headend platforms.		12.1(12.5)EC	12.1(13)EC1
12.1EV	Early Deployment Release	12.1(10)EV1b		12.1(10)EV4
12.1EW	Early deployment for the Cisco 4000 series			12.1(12c)EW
12.1(1)EX	Catalyst 6000 support			12.1(8b)E14
12.1(10)EX	Early deployment for the Cisco 7300 series			12.1(13)EX
12.1EY	Cat8510c, Cat8510m, Cat8540c, Cat8540m, LS1010	Not Scheduled		
		Upgrade recommended to 12.1(19)E		
12.1EZ	Early Deployment (ED): special image	12.1(6)EZ8		
	Early	Not Scheduled		

12.1T	Deployment(ED): VPN, Distributed Director, various platforms	Upgrade recommended to 12.2(10)
12.1XA	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(10)
12.1XB	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(10)
12.1XC	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(10)
12.1XD	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(10)
12.1XF	Early Deployment (ED): 811 and 813 (c800 images)	Not Scheduled
		Upgrade recommended to 12.2(10)
12.1XG	Early Deployment (ED): 800, 805, 820, and 1600	Not Scheduled
		Upgrade recommended to 12.2(8)T
12.1XH	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(10)
	Early	Not Scheduled

12.1XI	Deployment (ED): limited platforms	Upgrade recommended to 12.2(10)
12.1XJ	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended
12.1XK	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended
12.1XL	Early Deployment (ED): limited platforms	Not Scheduled
		Upgrade recommended to 12.2(10)
12.1XM	Short-lived early deployment release	Not Scheduled
		Upgrade recommended to 12.2(8)T
12.1XP	Early Deployment (ED): 1700 and SOHO	Not Scheduled
		Upgrade recommended
12.1XQ	Short-lived early deployment release	Not Scheduled
		Upgrade recommended to 12.2(10)
12.1XR	Short-lived early deployment release	End of Engineering
		Migrate recommended to 12.2(8)T
12.1XS	Short-lived early deployment	Not Scheduled

	release	Update recommended
12.1XT	Early Deployment (ED): 1700 series	Not Scheduled
		Upgrade recommended
12.1XU	Early Deployment (ED): limited platforms	End of Engineering
		Upgrade recommended
12.1XV	Short-lived early deployment release	Not Scheduled
		Upgrade recommended to 12.2(8)T
12.1XW	Short-lived early deployment release	Not Scheduled
		Upgrade recommended to 12.3
12.1XX	Short-lived early deployment release	Not Scheduled
		Upgrade recommended
12.1XY	Short-lived early deployment release	Not Scheduled
		Upgrade recommended
12.1XZ	Short-lived early deployment release	Not Scheduled
		Upgrade recommended
12.1YA	Short-lived early deployment release	Not Scheduled
		Upgrade recommended

12.1YB	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended		
12.1YC	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.2(8)T		
12.1YD	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.2(8)T		
12.1YF	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.3		
12.2-based Releases		Rebuild	Interim**	Maintenance
12.2	General deployment release for all platforms	12.2(6g)	12.2(7.4)	12.2(10)
12.2B	Special train for 6400, 7200, 7400,ubr10k, ubr7200 series		12.2(7.6)B	12.2(15)B
12.2BX	Broadband Leased Line			12.2(15)BX
12.2BW	Early deployment release for 7200, 7400 and 7511 platforms			12.2(15)BW

12.2DA	xDSL support for 6100 and 6200 platforms	12.2(9.4)DA		12.2(10)DA
12.2S	Core ISP Support		12.2(7.4)S	12.2(14)S
12.2T	Technology Train		12.2(7.4)T	12.2(8)T
12.2XA	SPLOB	Not Scheduled		
		Upgrade recommended to 12.2(8)T		
12.2XB	Short-lived early deployment release	12.2(2)XB7		
12.2XD	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.2(8)T		
12.2XE	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.2(8)T		
12.2XH	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.2(8)T		
12.2XQ	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to 12.2(11)T		
12.2XZ	Short-lived early deployment release	12.2(4)XZ5		

12.2YA	Short Lived Release	12.2(4)YA3		
12.2YC	Short Lived Release	12.2(2)YC4		
12.2ZN	Short Lived Release			12.2(15)ZN
12.3 and 12.3T images are not affected				
Notes				
<p>* All dates are estimates and subject to change.</p> <p>** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.</p>				

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

☐ Workarounds

Workarounds are described in this section.

Cisco IOS

There are methods available to mitigate the exposure. You can combine these methods or use them individually.

- Prevent IOS from processing NTP queries at all. Depending on whether you are acting as a server or a client, the configuration is different. Each configuration is described below:
If you are acting as a server only, and will not be synchronized by anyone else, then you can use the following configuration:

```
ntp access-group serve-only 20
access-list 20 permit any
```

The configuration above allows any peer to send an NTP request. If required, it is possible to limit allowed clients. In that case, ACL 20 can be modified to include only legitimate clients as in the following example

```
ntp access-group serve-only 20
access-list 20 permit <ntp client #1>
access-list 20 permit <ntp client #2>
```

If you are acting as a client only, then you can use the following configuration:

```
ntp server <ntp server #1>
ntp server <ntp server #2>
ntp access-group peer 10
access-list 10 permit host <ntp server #1>
access-list 10 permit host <ntp server #2>
```

The configuration above allows this device to be synchronized by either of the servers. Note that this will not prevent control packets from being executed, therefore you will only limit your exposure. However, only control packets sent by the servers will be processed.

If you are acting as a server and as a client, then you can use the following configuration:

```
ntp server <ntp server #1>
ntp server <ntp server #2>
ntp access-group peer 10
ntp access-group serve-only 20
access-list 10 permit host <ntp server #1>
access-list 10 permit host <ntp server #2>
access-list 20 permit <ntp client #1>
access-list 20 permit <ntp client #2>
```

The configuration above allows the router to respond to any NTP request and it will allow it to be synchronized by the given servers. Note that this will not prevent control packets from being executed, therefore you will only limit your exposure. However, only control packets sent by the servers will be processed.

- It is possible to mitigate the exposure by using ACLs and dropping all NTP packets that are not from the legitimate servers. This can be accomplished as follows:

```
access-list 10 permit <ntp server #1>
access-list 10 permit <ntp server #2>
access-list 10 deny any
!
ntp access-group peer 10
```

In the above example, <ntp server #1> and <ntp server #2> are addresses of peers or servers from which NTP packets will be accepted..

- Additionally, if you are not using NTP servers external from your network, you can drop all NTP packets on the network boundary. This can be done by integrating the following line to your existing ACL

```
access-list 101 deny udp any any eq ntp
```

If you do not have an existing ACL, the following ACL can be used on the network boundary to deny only ntp and permit the rest of the IP traffic

```
access-list 101 deny udp any any eq ntp
access-list 101 permit ip any any
```

For more detailed information regarding individual commands and additional examples, please refer to the following documentation:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd303.htm
- <http://www.cisco.com/public/cons/isp/essentials/>

MGC and Related Products

Cisco IP Manager

BTS 10200

Although the workaround was posted on the Bugtraq list we recommend installing the patch provided.

The users must follow the installation instructions that are part of the patch.

☐ **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.

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

☐ **Exploitation and Public Announcements**

This vulnerability was discovered by Przemyslaw Frasunek and it has been posted on the Bugtraq list on 2001-April-04. The full text of the mail can be seen at: <http://www.securityfocus.com/archive/1/174011>. This vulnerability is also described in CERT/CC vulnerability note VU#970472 available at <http://www.kb.cert.org/vuls/id/970472> .

Our initial response has been sent to Bugtraq on 2001-April-12 and can be seen at <http://www.securityfocus.com/archive/1/176137>.

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

☐ **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.

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

☐ **Distribution**

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020508-ntp-vulnerability.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
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

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

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

☐ **Revision History**

--	--	--

Revision 2.1	2003-Oct-02	Updated and added IOS release information in "Software Versions and Fixes" section.
Revision 2.0	2003-Sept-22	New bug has been added. Fixed IOS releases are updated. Patch for Solaris 8 is added.
Revision 1.5	2002-May-16	The syntax of an access-list in the Workarounds section was corrected.
Revision 1.4	2002-May-15	Removed "Use NTP with authentication" workaround.
Revision 1.3	2002-May-13	Updated Details section and added a URL to CERT/CC vulnerability note VU#970472 in Exploitation and Public Announcements.
Revision 1.2	2002-May-10	Updated products not affected to include Cisco Secure PIX Firewall. Also, updated the first workaround technique for Cisco IOS, which is preventing IOS from processing NTP queries.
Revision 1.1	2002-May-09	Added Products Not Affected.
Revision 1.0	2002-May-08	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 Web site 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)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

© 2010 - 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)