

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – NTP Issue</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2001 April 12</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Cisco Security Procedures</u>	2

Cisco Security Notice: Response to BugTraq – NTP Issue

Revision 1.0

Last Updated 2001 April 12

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/1/174011> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/176137> .

```
To: BugTraq
Subject: IOS and NTP
Date: Apr 12 2001 9:18AM
Author: Damir Rajnovic <gaus cisco com>
Message-ID: <4.2.0.58.20010412090616.07246bf0@amsterdam.cisco.com>
In-Reply-To: <20010411184348.K413@tigerteam.net>
```

Hi there,

```
At 18:43 11/04/2001 +0700, Fyodor wrote:
>Cisco IOS (at least 11.x series) _IS_ vulnerable (tested, confirmed). Earlier
>versions are presumably vulnerable too. Haven't tested IOS 12.x but it may have
>the same bug inherited as well (unless cisco folks found the problem and fixed
>it silently).
```

Despite what Fyodor said, we were unable to get IOS crash. Admittedly, we have not tested all IOS releases but we did test: 10.3, 11.0, 12.0 and 12.1.

Our finding is that we were unable to crash IOS by using the exploit which has been posted on the Bugtraq.

However, we can not rule out the possibility that certain IOS release, on a given HW with a particular configuration will crash. So, in the mean time, as a precaution, we advise all customers to insert the following

line into the configuration:

```
ntp access-group serve-only
```

This will prevent the router from processing NTP control requests.

Cheers,

Gaus

=====

Damir Rajnovic <psirt cisco com>, PSIRT Incident Manager, Cisco Systems
<http://www.cisco.com/warp/public/707/sec_incident_response.shtml>

Phone: +44 7715 546 033

4 The Square, Stockley Park, Uxbridge, MIDDLESEX UB11 1BN, GB

=====

There is no insolvable problems. Question remains: can you
accept the solution?

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. 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 © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.