Tools & Resources

Bug Search

Bug Search CSCum52148 Help | [+] Feedback

Distributed reflective denial-of-service vulnerability on NTP server
CSCum52148

Description

Customer Visible

Save Bug

Open Support Case

Symptom:
A vulnerability in Network Time Protocol (NTP) package of Cisco IOS and Cisco NX-OS Software could allow an unauthenticated, remote attacker to
cause a Denial of Service (DoS) condition on an affected device.

The vulnerability is due to processing of MODE_PRIVATE (Mode 7) NTP control messages which have a large
amplification vector. An attacker could exploit this vulnerability by
sending Mode 7 control requests to NTP servers and observing responses amplified up to 5500 times in size. An exploit could allow the attacker to cause a Denial of Service (DoS) condition where the
affected NTP server is forced to process and respond with large response data.

Conditions:
Cisco NX-OS Software is vulnerable to attacks utilizing Mode 7 NTP requests.
Mode 7 requests can have amplification vector up to 5500.

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
ntp peer
ntp server
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#

Information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS and NX-OS Software Reference Guide" at the following link:
http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Workaround:
There are no solid 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.

Additionally, "serve-only" keyword added to the NTP access-group will limit the exposure of the server to only respond to valid queries.

For additional information on NTP access control groups, consult the document titled "Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x" at the following link:
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/system_management/configuration/guide/sm_3ntp.html

* 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 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

- Filtering untrusted sources to the device.

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. 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.

- Rate Limiting the traffic to the device

Note: Since the NTP Amplification DoS attacks rely on sending relatively small amount of NTP requests in order to solicit large, amplified responses from the server, this workaround has only limited application.

Additional information on the configuration and use of the CoPP feature can be found in the documents, "Control Plane Policing Implementation Best Practices" and "Understand CoPP on Nexus 7000 Series Switches" at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and
http://www.cisco.com/en/US/products/ps9402/products_tech_note09186a0080c01155.shtml

Further Problem Description:
The vulnerability comes from a shortcoming in RFC5905 that allows processing of optional Mode 7 command requests by NTP servers.

In summary, the attack is based on the premise of processing Mode 7 (MODE_PRIVATE) requests from the
clients. While the requests are small (for example, in case of Mode 7 only 8 bytes long), the response can grow up to 5500 times in amplification factor
size.

PSIRT Evaluation:
The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are
5/4.5:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?
dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:W/RC:C
CVE ID CVE-2013-5211 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at:
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5211

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Was the description about this Bug Helpful? *(0)*

Details

Last Modified: Feb 12,2014

Status: Open

Severity: 6 Enhancement

Product: Cisco Nexus 7000 Series Switches

Support Cases: 0

Known Affected Releases: *(1)*
6.0(2)

Known Fixed Releases: *(0)*

Download software for Cisco Nexus 7000 Series Switches

Community Discussion on CSCum52148 - Cisco Support Community *0 Discussion(s)*

Start Community Discussion