Tools & Resources

Bug Search

Bug Search CSCum76937 Help | Feedback

CUCM Distributed denial-of-service vulnerability on NTP server
CSCum76937

Description

Symptom: Cisco Unified Communications Manager (CallManager) includes a version of ntpd that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

CVE-2013-5211

This bug was opened to address the potential impact on this product.

Conditions: Device configured to use/broadcast NTP.

Workaround: Use ACLs to restrict incoming NTP traffic from outside of the network.

Modify /etc/ntp.conf:

A possible workaround is to modify the /etc/ntp.conf file to include the noquery
entry. NTP needs to be restarted after this change.

NTP config before:

[root@cucm911ccnapub ~]# vi /etc/ntp.conf

~~~

Leave access open because a server may be added to a cluster
strictly by its host name in the UCM Administration GUI and Cluster
Manager may not yet have updated /etc/hosts with the IP address,
thereby temporarily preventing secondary node access.
restrict default

~~~

Modified NTP:

Leave access open because a server may be added to a cluster
strictly by its host name in the UCM Administration GUI and Cluster
Manager may not yet have updated /etc/hosts with the IP address,
thereby temporarily preventing secondary node access.
restrict default noquery

~~~

Restart NTP from admin.

admin:utils ntp restart

More Info: Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html

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

Customer Visible

Save Bug

Open Support Case
~~~

Was the description about this Bug Helpful? *(1)*

Details

Last Modified: Feb 12,2014

Status: Open

Severity: 2 Severe

Product: Cisco Unified Communications Manager (CallManager)

Support Cases: 0

Known Affected Releases: *(3)*

8.6(2)
8.5(1)
9.1(2)

Known Fixed Releases: *(0)*

Download software for Cisco Unified Communications Manager (CallManager)

Community Discussion on CSCum76937 - Cisco Support Community *1 Discussion(s)*

CSCum76937 - CUCM Distributed denial-of-service vulnerability on NTP server
good suggestion, thanks! yes, there IS an iptables in the device itself, but it's pretty generically limited in what it can do.

Author: sweeny | **Posted:** Feb 3, 2014 | **Latest activity:** Feb 3, 2014

Start Community Discussion