

Cisco Security Advisory: Cisco CNS Network Registrar Denial of Service Vulnerability

Document ID: 63413

Advisory ID: cisco-sa-20041202-cnr

<http://www.cisco.com/warp/public/707/cisco-sa-20041202-cnr.shtml>

Revision 1.1

Last Updated 2004 December 07 1930 UTC (GMT)

For Public Release 2004 December 02 1600 UTC (GMT)

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

[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

Cisco CNS Network Registrar Domain Name Service /Dynamic Host Configuration Protocol (DNS/DHCP) server for the Windows Server platforms is vulnerable to a Denial of Service attack when a certain crafted packet sequence is directed to the server. Cisco has made free software available to address this vulnerability for all affected customers.

The vulnerabilities are documented as the following Cisco Bug IDs: CSCeg27625 and CSCeg27614.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20041202-cnr.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Cisco CNS Network Registrar for Windows NT server and Windows 2000

Two issues are described in this advisory CSCeg27625 and CSCeg27614. Cisco CNS Network Registrar version 6.0 through 6.1.1.3 are affected by CSCeg27625. However, all versions up to and including version 6.1.1.3 are also affected by CSCeg27614.

Products Confirmed Not Vulnerable

The following Cisco Network Registrar products are not vulnerable to the issues described in this advisory:

- Cisco Network Registrar for Unix
- Cisco Network Registrar for Linux

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

Cisco CNS Network Registrar is a DNS and DHCP server installed on Windows NT servers and Windows 2000 servers. Two separate vulnerabilities may impact system stability or availability if exploited. These issues are detailed below:

- **CSCeg27625** The Cisco CNS Network Registrar CCM (Central Configuration Management) server may consume almost 100% of the system CPU when a remote user ends a connection after sending a specific sequence of packets. The server agent must be restarted to clear this condition.
- **CSCeg27614** The Cisco CNS Network Registrar lock manager process may crash when the system receives an unexpected packet sequence. This will cause the CCM server to also fail. You must restart the server agent to resume normal operations.

These issues are unrelated to the recent Cisco Security Advisory regarding Cisco IOS DHCP implementation. <http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp.shtml> These issues are also unrelated to the recent UNIRAS advisory regarding DNS.

Impact

Exploitation of either CSCeg27625 or CSCeg27614 can result in a denial of service attack, stemming from system resource starvation or unavailability.

Software Versions and Fixes

The two issues are fixed in the 6.1.1.4 patch release. Releases are available for download to registered customers on CCO at: <http://www.cisco.com/cgi-bin/Software/Tablebuild/tablebuild.pl/nr-eval>

Customers who are using Cisco Network Registrar 5.5 versions must request a new license key for the Cisco CNS Network Registrar 6.1.1.x release before obtaining the patched 6.1.1.4 release from CCO. Version 5.5 license keys are incompatible with the Cisco CNS Network Registrar 6.0 or 6.1 software releases. To request a new license key, any customer wishing to upgrade version 5.5 to version 6.1 software should send an electronic mail message to cnr-psirt-update@cisco.com, and provide the customer name, address, contact name and existing version 5.5 license key string in the body of the message along with a line indicating CNR PSIRT upgrade for Windows request . A new license key will be dispatched via email to the requestor, allowing them to install and upgrade to the patched 6.1.1.4 release using the new license key.

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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) for assistance. 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

Workarounds

These vulnerabilities can be mitigated by placing access lists on adjacent network devices such as routers or firewalls to block inbound connections to all high or ephemeral port numbers, including the CCM port.

If remote access to the Cisco CNS Network Registrar is required, it is recommended that trusted hosts be explicitly permitted in access control lists, and all other connection attempts blocked. Remote connection CLI ports are tcp 2785 & tcp 2786, and the default port number for CCM is tcp1234, which can also be configured to a different port number. Access lists permitting selective access to these ports from trusted IP addresses can mitigate this vulnerability.

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

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.

Exploitation and Public Announcements

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

The discovery and documentation of this vulnerability was conducted by the Qualys Security Research Team. More information about the Qualys Security Research Team can be found at their website:

<http://www.qualys.com>

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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20041202-cnr.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-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- 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 1.1	2004-December-07	Corrected transposed digits in workaround section of port numbers 2875 to 2785 and 2876 to 2786.
Revision 1.0	2004-December-02	Initial public release.

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>.

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Dec 07, 2004

Document ID: 63413
