

# Cisco Security Advisory: Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks

Advisory ID: cisco-sa-20080708-dns

<http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>

## Revision 2.1

Last Updated 2008 September 09 2230 UTC (GMT)

For Public Release 2008 July 08 1800 UTC (GMT)

---

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

---

## Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>.

This security advisory is being published simultaneously with announcements from other affected organizations.

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

### ☐ **Affected Products**

Products that cache DNS responses and process DNS messages with the recursion desired (RD) flag set may be vulnerable to a DNS cache poisoning attack depending on implementation of the DNS protocol. Products that process DNS messages with the RD flag set will attempt to answer the question asked on behalf of the client. A product is only affected if using a vulnerable implementation of the DNS protocol, the DNS server functionality for the product is enabled, and the DNS feature for the product is configured to process recursive DNS query messages.

### ☐ **Vulnerable Products**

The following Cisco products are capable of acting as DNS servers and have been found to have the DNS implementation weakness that makes some types of DNS cache poisoning attacks more likely to succeed:

- **Cisco IOS Software**

A device that is running Cisco IOS Software will be affected if it is running a vulnerable

version and if it is acting as a DNS server.

All Cisco IOS Software releases that support the DNS server functionality and that have not had their DNS implementation improved are affected. For information about specific fixed versions, please refer to the [Software Versions and Fixes](#) section.

A device that is running Cisco IOS Software is configured to act as a DNS server if the command **ip dns server** is present in the configuration. This command is not enabled by default.

- **Cisco Network Registrar**

All Cisco Network Registrar versions are affected, and DNS services are enabled by default.

The DNS server on CNR is enabled via the command-line interface (CLI) commands **server dns enable start-on-reboot** or **dns enable start-on-reboot** or via the web management interface in the Servers page by selecting the appropriate "Start," "Stop," or "Reload" button.

- **Cisco Application and Content Networking System**

All Cisco Application and Content Networking System (ACNS) versions are affected; DNS services are disabled by default.

ACNS is configured to act as a DNS server if the command **dns enable** is present in the configuration.

- **Cisco Global Site Selector Used in Combination with Cisco Network Registrar**

The Cisco Global Site Selector (GSS) is affected when it is used in combination with Cisco Network Registrar software to provide a more complete DNS solution. Fixed software would come in the form of an update of the Cisco Network Registrar software rather than an update of the GSS software.

## ☐ **Products Confirmed Not Vulnerable**

Products that do not offer DNS server capabilities are not affected by this vulnerability.

The Cisco GSS by itself is not affected by this vulnerability. However, it is affected when it is used with Cisco Network Registrar software.

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

## ☐ Details

The Domain Name System is an integral part of networks that are based on TCP/IP such as the Internet. Simply stated, the Domain Name System is a hierarchical database that contains mappings of hostnames and IP addresses. The DNS protocol is part of the TCP/IP protocol suite and allows DNS clients to query the DNS database to resolve hostnames to IP addresses.

A DNS server is an application that implements the DNS protocol and that has the ability to respond to queries made by DNS clients. When handling a query from a DNS client, a DNS server can look into its portion of the global DNS database (if the query is for a portion of the DNS database for which the DNS server is authoritative), or it can relay the query to other DNS servers (if it is configured to do so and if the query is for a portion of the DNS database for which the DNS server is not authoritative.)

Because of the processing time and bandwidth that is associated with handling a DNS query, most DNS servers locally store responses that are received from other DNS servers. The area where these responses are stored locally is called a "cache." Once a response is stored in a cache, the DNS server can use the locally stored response for a certain time (called the "time to live") before having to query DNS servers again to refresh the local (cached) copy of the response.

A DNS cache poisoning attack is an attack in which an entry in the DNS cache of a DNS server is changed so the IP address associated with a hostname in the cache does not point to the correct place. For example, if `www.example.com` is mapped to the IP address `192.168.0.1` and this mapping is present in the cache of a DNS server, an attacker who succeeds in poisoning the DNS cache of this server may be able to map `www.example.com` to `10.0.0.1` instead. If this happens, a user who is trying to visit `www.example.com` may end up contacting the wrong web server.

Although DNS cache poisoning attacks are not new, a security researcher recently presented a technique that allows an attacker to mount successful DNS cache poisoning attacks with low complexity tools and low traffic requirements. This technique exploits a weakness in most implementations of the DNS protocol. The fundamental implementation weakness is that the DNS transaction ID and source port number used to validate DNS responses are not sufficiently randomized and can easily be predicted, which allows an attacker to create forged responses to DNS queries that will match the expected values. The DNS server will consider such responses to be valid.

The following Cisco products that offer DNS server functionality have been found to be susceptible to DNS cache poisoning attacks:

- Cisco IOS Software: The vulnerability documented in Cisco bug ID [CSCso81854](#) ( [registered](#) customers only) .
- Cisco Network Registrar: The vulnerability documented in Cisco bug ID [CSCsq01298](#) ( [registered](#) customers only) .
- Cisco Application and Content Networking System (ACNS): The vulnerability documented in Cisco bug ID [CSCsq21930](#) ( [registered](#) customers only) .

This vulnerability has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2008-1447.

## Port Address Translation Considerations

Port Address Translation (PAT) is a form of Network Address Translation (NAT) that allows multiple hosts in a private network to access a public network using a single, public IP address. This is accomplished by rewriting layer 4 information, specifically TCP and UDP source port numbers and checksums, as packets from the private network traverse a network device that is performing PAT. PAT is configured by network administrators and performed by network devices such as firewalls and routers in situations where public IP addresses are limited.

After the initial multi-vendor DNS advisory was published on July 8th, 2008 it was discovered that in some cases the fixes to DNS implementations to use random source ports when sending DNS queries could be negated when such queries traverse PAT devices. The reason for this is that in these cases the network device performing PAT uses a predictable source port allocation policy, such as incremental allocation, when performing the layer 4 rewrite operation that is necessary for PAT. Under this scenario, the fixes made by DNS vendors can be greatly diminished because, while DNS queries seen on the inside network have random source port numbers, the same queries have potentially predictable source port numbers when they leave the private network, depending on the type of traffic that transits through the device.

Several Cisco products are affected by this issue, and if DNS servers are deployed behind one of these affected products operating in PAT mode then the DNS infrastructure may still be at risk even if source port randomization updates have been applied to the DNS servers.

The affected Cisco products, and the respective Cisco bugs that have been created to track the issue, are the following:

<b>Product</b>	<b>Cisco Bug ID</b>
Cisco PIX (6.3.x and earlier)	<a href="#">CSCsr28354</a> ( <a href="#">registered</a> customers only)

Cisco ASA and Cisco PIX (7.0.x and later)	<a href="#">CSCsr28008</a> ( <a href="#">registered customers only</a> )
Firewall Services Module (FWSM)	<a href="#">CSCsr29124</a> ( <a href="#">registered customers only</a> )
Cisco IOS	<a href="#">CSCsr29691</a> ( <a href="#">registered customers only</a> )
Cisco Content Switching Module (CSM)	<a href="#">CSCsr61220</a> ( <a href="#">registered customers only</a> )
Cisco Application Control Engine (ACE) Module	<a href="#">CSCsr98689</a> ( <a href="#">registered customers only</a> )
Cisco Application Control Engine (ACE) Appliance	<a href="#">CSCsu10546</a> ( <a href="#">registered customers only</a> )

Fixed software information for these bugs will not be added to this document. Instead, customers should use their regular support channels or the bug tracking features of the Bug Toolkit application on [cisco.com](http://cisco.com) to obtain fixed software information.

With the exception of the ACE module and the ACE appliance, the above products use an incremental source port allocation policy when performing the source port rewrite operation that is needed for PAT. In the case of Cisco IOS, the original source port will be tried first, but if that port is already allocated and in use for an existing PAT translation then a new port will be incrementally assigned.

The ACE module and the ACE appliance do not use an incremental source port allocation. However, they use a hash algorithm that may make predictable the chosen source port number during PAT operation.

Note that traditional NAT, i.e. allocating one public IP address for each private IP address, is not affected by this problem because, unlike PAT, NAT only rewrites layer 3 information and does not modify layer 4 header information of packets traversing the NAT device.

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

## ☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

<b><u><a href="#">CSCso81854</a></u>, <u><a href="#">CSCsq01298</a></u>, <u><a href="#">CSCsq21930</a></u></b>					
<b>Calculate the environmental score of <u><a href="#">CSCso81854/CSCsq01298/CSCsq21930</a></u></b>					
<b>CVSS Base Score - 6.4</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	Partial	Partial
<b>CVSS Temporal Score - 5.3</b>					
Exploitability	Remediation Level		Report Confidence		
Functional	Official-Fix		Confirmed		

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

## ☐ Impact

Successful exploitation of the vulnerability described in this document may result in invalid hostname-to-IP address mappings in the cache of an affected DNS server. This may lead users of this DNS server to contact the wrong provider of network services. The ultimate impact varies

greatly, ranging from a simple denial of service (for example, making [www.example.com](http://www.example.com) resolve to 127.0.0.1) to phishing and financial fraud.

[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.

### Cisco IOS Software

Each row of the Cisco IOS Software table (below) names a Cisco IOS Software release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

<b>Major Release</b>	<b>Availability of Repaired Releases</b>	
<b>Affected 12.0-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.0	Not Vulnerable	
12.0DA	Not Vulnerable	

12.0DB	Releases prior to 12.0(7)DB are vulnerable, release 12.0(7)DB and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.0DC	Releases prior to 12.0(7)DC are vulnerable, release 12.0(7)DC and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.0S	Not Vulnerable	
12.0SC	Not Vulnerable	
12.0SL	Not Vulnerable	
12.0SP	Not Vulnerable	
12.0ST	Not Vulnerable	
12.0SX	Not Vulnerable	
12.0SY	Not Vulnerable	
12.0SZ	Not Vulnerable	
12.0T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)

12.0W	Not Vulnerable	
12.0WC	Vulnerable; contact TAC	
12.0WT	Not Vulnerable	
12.0XA	Not Vulnerable	
12.0XB	Not Vulnerable	
12.0XC	Not Vulnerable	
12.0XD	Not Vulnerable	
12.0XE	Note: Releases prior to 12.0(7) XE1 are vulnerable, release 12.0(7) XE1 and later are not vulnerable;	
12.0XF	Not Vulnerable	
12.0XG	Not Vulnerable	
12.0XH	Not Vulnerable	
12.0XI	Not Vulnerable	
12.0XJ	Not Vulnerable	

12.0XK	Releases prior to 12.0(7)XK2 are vulnerable, release 12.0(7)XK2 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.0XL	Not Vulnerable	
12.0XM	Not Vulnerable	
12.0XN	Not Vulnerable	
12.0XQ	Not Vulnerable	
12.0XR	Releases prior to 12.0(7)XR1 are vulnerable, release 12.0(7)XR1 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.0XS	Not Vulnerable	
12.0XV	Not Vulnerable	
12.0XW	Not Vulnerable	
<b>Affected 12.1-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>

12.1	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.1AA	Not Vulnerable	
12.1AX	Not Vulnerable	
12.1AY	Releases prior to 12.1(22)AY1 are vulnerable, release 12.1(22)AY1 and later are not vulnerable;	12.1(22)EA11
12.1AZ	Not Vulnerable	
12.1CX	Not Vulnerable	
12.1DA	Not Vulnerable	
12.1DB	Releases prior to 12.1(4)DB1 are vulnerable, release 12.1(4)DB1 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.1DC	Releases prior to 12.1(4)DC2 are vulnerable, release 12.1(4)DC2 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)

12.1E	Not Vulnerable	
12.1EA	Releases prior to 12.1(11)EA1 are vulnerable, release 12.1(11)EA1 and later are not vulnerable;	12.1(22)EA11
12.1EB	Not Vulnerable	
12.1EC	Not Vulnerable	
12.1EO	Not Vulnerable	
12.1EU	Not Vulnerable	
12.1EV	Not Vulnerable	
12.1EW	Not Vulnerable	
12.1EX	Note: Releases prior to 12.1(8a)EX are vulnerable, release 12.1(8a)EX and later are not vulnerable;	
12.1EY	Not Vulnerable	
12.1EZ	Not Vulnerable	
12.1GA	Not Vulnerable	

12.1GB	Not Vulnerable	
12.1T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.1XA	Not Vulnerable	
12.1XB	Not Vulnerable	
12.1XC	Releases prior to 12.1(1)XC1 are vulnerable, release 12.1(1)XC1 and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.1XD	Not Vulnerable	
12.1XE	Not Vulnerable	
12.1XF	Not Vulnerable	
12.1XG	Not Vulnerable	
12.1XH	Not Vulnerable	
12.1XI	Not Vulnerable	
12.1XJ	Not Vulnerable	
12.1XK	Not Vulnerable	

12.1XL	Not Vulnerable	
12.1XM	Not Vulnerable	
12.1XN	Not Vulnerable	
12.1XO	Not Vulnerable	
12.1XP	Not Vulnerable	
12.1XQ	Not Vulnerable	
12.1XR	Not Vulnerable	
12.1XS	Not Vulnerable	
12.1XT	Not Vulnerable	
12.1XU	Not Vulnerable	
12.1XV	Not Vulnerable	
12.1XW	Not Vulnerable	
12.1XX	Not Vulnerable	
12.1XY	Not Vulnerable	
12.1XZ	Not Vulnerable	
12.1YA	Not Vulnerable	

12.1YB	Not Vulnerable	
12.1YC	Not Vulnerable	
12.1YD	Not Vulnerable	
12.1YE	Note: Releases prior to 12.1(5) YE1 are vulnerable, release 12.1(5) YE1 and later are not vulnerable;	12.4(19a) 12.4(19b)
12.1YF	Not Vulnerable	
12.1YG	Not Vulnerable	
12.1YH	Not Vulnerable	
12.1YI	Not Vulnerable	
12.1YJ	Not Vulnerable	
<b>Affected 12.2-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.2	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2B	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)

12.2BC	Not Vulnerable	
12.2BW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2BY	Releases prior to 12.2(8)BY are vulnerable, release 12.2(8)BY and later are not vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Vulnerable; contact TAC	
12.2DA	Not Vulnerable	
12.2DD	Not Vulnerable	
12.2DX	Not Vulnerable	
12.2EU	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	

12.2EX	Not Vulnerable	
12.2EY	Not Vulnerable	
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Not Vulnerable	
12.2IXA	Not Vulnerable	
12.2IXB	Not Vulnerable	
12.2IXC	Not Vulnerable	
12.2IXD	Not Vulnerable	
12.2IXE	Not Vulnerable	
12.2IXF	Not Vulnerable	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	

12.2S	Not Vulnerable	
12.2SB	Not Vulnerable	
12.2SBC	Not Vulnerable	
12.2SCA	Not Vulnerable	
12.2SE	Not Vulnerable	
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Not Vulnerable	
12.2SED	Not Vulnerable	
12.2SEE	Not Vulnerable	
12.2SEF	Not Vulnerable	
12.2SEG	Not Vulnerable	
12.2SG	Not Vulnerable	
12.2SGA	Not Vulnerable	
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	

12.2SO	Not Vulnerable	
12.2SRA	Not Vulnerable	
12.2SRB	Not Vulnerable	
12.2SRC	Not Vulnerable	
12.2SU	Not Vulnerable	
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Not Vulnerable	
12.2SXA	Not Vulnerable	
12.2SXB	Not Vulnerable	
12.2SXD	Not Vulnerable	
12.2SXE	Not Vulnerable	
12.2SXF	Not Vulnerable	

12.2SXH	Not Vulnerable	
12.2SXI	Not Vulnerable	
12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2TPC	Releases prior to 12.2(8)TPC10d are vulnerable, release 12.2(8) TPC10d and later are not vulnerable;	
12.2UZ	Not Vulnerable	
12.2XA	Not Vulnerable	
12.2XB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2XD	Not Vulnerable	
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	

12.2XG	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2XH	Not Vulnerable	
12.2XI	Not Vulnerable	
12.2XJ	Not Vulnerable	
12.2XK	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2XL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2XM	Not Vulnerable	
12.2XN	Not Vulnerable	
12.2XNA	Not Vulnerable	
12.2XO	Not Vulnerable	
12.2XQ	Not Vulnerable	
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	
12.2XT	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)

12.2XU	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2XV	Not Vulnerable	
12.2XW	Not Vulnerable	
12.2YA	Not Vulnerable	
12.2YB	Not Vulnerable	
12.2YC	Not Vulnerable	
12.2YD	Not Vulnerable	
12.2YE	Not Vulnerable	
12.2YF	Not Vulnerable	
12.2YG	Not Vulnerable	
12.2YH	Not Vulnerable	
12.2YJ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2YK	Not Vulnerable	
12.2YL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)

12.2YM	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2YN	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2YO	Vulnerable; migrate to any release in 12.2SY	12.2(18)SXF15; Available on 08-AUG-08
12.2YP	Not Vulnerable	
12.2YQ	Not Vulnerable	
12.2YR	Not Vulnerable	
12.2YS	Not Vulnerable	
12.2YT	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2YU	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2YV	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2YW	Not Vulnerable	
12.2YX	Not Vulnerable	
12.2YY	Not Vulnerable	
12.2YZ	Not Vulnerable	

12.2ZA	Not Vulnerable	
12.2ZB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2ZC	Not Vulnerable	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2ZF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2ZG	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08
12.2ZH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08
12.2ZJ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.2ZL	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08

12.2ZP	Not Vulnerable	
12.2ZU	Not Vulnerable	
12.2ZY	Not Vulnerable	
12.2ZYA	Not Vulnerable	
<b>Affected 12.3-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.3	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3B	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3BC	Not Vulnerable	
12.3BW	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	

12.3JK	Not Vulnerable	
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	
12.3T	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3TPC	Vulnerable; contact TAC	
12.3VA	Vulnerable; contact TAC	
12.3XA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08
12.3XB	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3XC	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08
12.3XD	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)

12.3XE	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08
12.3XF	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3XG	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08
12.3XH	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3XI	Vulnerable; contact TAC	
12.3XJ	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX12 12.4(20)T; Available on 11-JUL-08
12.3XK	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3XQ	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3XR	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08

12.3XS	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b)
12.3XU	Not Vulnerable	
12.3XW	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX12 12.4(20)T; Available on 11-JUL-08
12.3XY	Not Vulnerable	
12.3YA	Vulnerable; first fixed in <a href="#">12.4</a>	12.4(19a) 12.4(19b) 12.4(20)T; Available on 11-JUL-08
12.3YD	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.3YF	Vulnerable; first fixed in <a href="#">12.3YX</a>	12.3(14)YX12 12.4(20)T; Available on 11-JUL-08
12.3YG	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.3YH	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.3YI	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.3YJ	Not Vulnerable	
12.3YK	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08

12.3YM	Releases prior to 12.3(14)YM12 are vulnerable, release 12.3(14)YM12 and later are not vulnerable;	12.3(14)YM12
12.3YQ	Not Vulnerable	
12.3YS	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.3YT	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.3YU	Vulnerable; first fixed in <a href="#">12.4XB</a>	
12.3YX	12.3(14)YX12	12.3(14)YX12
12.3YZ	Vulnerable; contact TAC	
<b>Affected 12.4-Based Releases</b>	<b>First Fixed Release</b>	<b>Recommended Release</b>
12.4	12.4(18b) 12.4(19a) 12.4(19b) 12.4(21)	12.4(19a) 12.4(19b)
12.4JA	Not Vulnerable	
12.4JK	Not Vulnerable	

12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JMC	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	12.4(15)MD	12.4(15)MD
12.4MR	12.4(19)MR	12.4(19)MR
12.4SW	Vulnerable; contact TAC	
12.4T	12.4(15)T6  12.4(20)T; Available on 11- JUL-08	12.4(20)T; Available on 11-JUL-08
12.4XA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.4XB	12.4(2)XB10	
12.4XC	Vulnerable; contact TAC	
12.4XD	12.4(4)XD11; Available on 31- JUL-08	12.4(20)T; Available on 11-JUL-08
12.4XE	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.4XF	Not Vulnerable	

12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08
12.4XK	Not Vulnerable	
12.4XL	12.4(15)XL2	12.4(15)XL2
12.4XM	12.4(15)XM1	12.4(15)XM1
12.4XN	Vulnerable; contact TAC	
12.4XQ	Vulnerable; contact TAC	
12.4XT	Vulnerable; contact TAC	
12.4XV	Vulnerable; contact TAC	
12.4XW	12.4(11)XW8	12.4(11)XW6
12.4XY	12.4(15)XY3	
12.4XZ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T; Available on 11-JUL-08

## Cisco Network Registrar

Affected Release Train	First Fixed Release

Pre-6.1.x	Software has reached End of Support status. Customers running pre-6.1.x versions are advised to upgrade to a newer version as soon as possible.
6.1.x	Upgrade to 6.2.4.1; available now
6.2.x	6.2.4.1; available now
6.3.x	6.3.1.5; available now
7.0.x	7.0.1; available late September 2008

Cisco Network Registrar software is available for download at <http://www.cisco.com/cgi-bin/Software/Tablebuild/tablebuild.pl/nr-eval?psrtdcat20e2>

## Cisco Application and Content Networking System

This issue is fixed in version 5.5.11.2 of Cisco ACNS software, which is available now.

Cisco ACNS 5.5 software is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/acns55?psrtdcat20e2>.

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

## Workarounds

There are no workarounds.

Additional information about identification and mitigation of attacks against DNS is in the Cisco Applied Intelligence white paper "DNS Best Practices, Network Protections, and Attack Identification," available at <http://www.cisco.com/web/about/security/intelligence/dns-bcp.html>.

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

## Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto: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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of 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 localized telephone numbers, and instructions and e-mail addresses for use in various languages.

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

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of malicious use of the vulnerability described in this advisory. Full technical details about the nature of the vulnerability are publicly available and the Metasploit project has published two modules that can exploit this vulnerability.

Although DNS cache poisoning attacks are not new, security researcher Dan Kaminsky of IOActive recently presented a technique that makes DNS cache poisoning attacks more likely to succeed. Cisco would like to thank Dan Kaminsky for notifying vendors about his findings.

Note that vulnerability information for Cisco IOS Software is being provided in this advisory outside of the announced publication schedule for Cisco IOS Software described at <http://www.cisco.com/go/psirt> due to industry-wide disclosure of the vulnerability.

The multi-vendor advisory published by US-CERT is available at <http://www.kb.cert.org/vuls/id/800113>  ("VU#800113 - Multiple DNS implementations vulnerable to cache poisoning").

[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 advisory is posted on Cisco's worldwide website at

<http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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.

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

## ☐ **Revision History**

Revision 2.1	2008-September 09	<p>Added Cisco bug IDs for the Cisco Application Control Engine (ACE) module and the Cisco ACE appliance to the "Port Address Translation Considerations" section since these devices may have a predictable source port allocation policy when doing PAT.</p> <p>Updated fixed software information and availability dates for Cisco Network Registrar and for Cisco Application and Content Networking System.</p>
Revision 2.0	2008-July-28	<p>Added a "Port Address Translation Considerations" section to highlight the problems and risks when DNS servers are behind network devices performing PAT, and to provide information and Cisco bug IDs for Cisco products that can perform PAT and that use predictable source port allocation policies when performing the layer 4 rewrite needed for PAT operation.</p> <p>Updated fixed software availability dates for Cisco Network Registrar.</p>

Revision 1.2	2008-July-25	Updated the "Exploitation and Public Announcements" section to indicate that full technical details and exploit code are publicly available. Added link to US-CERT Vulnerability Note.
Revision 1.1	2008-July-22	Fixed link to CVSS score calculator. Updated table of fixed software for Cisco Network Registrar. Mention that we are aware of public discussion of the details of the vulnerability. Updated availability information for ACNS software.
Revision 1.0	2008-July-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 website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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>.

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

---

## 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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)