

# Table of Contents

**Cisco Security Advisory: Cisco Content Service Switch 11000 Series DNS Negative Cache of Information Denial-of-Service Vulnerability.....1**

Document ID: 42486.....1

Revision 1.2.....1

Last Updated 2003 May 23 13:54 (GMT).....1

For Public Release 2003 April 30 08:00 (GMT).....1

Please provide your feedback on this document.....1

Summary.....1

Affected Products.....1

Details.....2

Impact.....2

Software Versions and Fixes.....3

Obtaining Fixed Software.....3

Workarounds.....4

Exploitation and Public Announcements.....4

Status of This Notice: FINAL.....4

Distribution.....4

Revision History.....5

Cisco Security Procedures.....5

# Cisco Security Advisory: Cisco Content Service Switch 11000 Series DNS Negative Cache of Information Denial-of-Service Vulnerability

Document ID: 42486

## Revision 1.2

Last Updated 2003 May 23 13:54 (GMT)

For Public Release 2003 April 30 08:00 (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Obtaining Fixed Software**  
**Workarounds**  
**Exploitation and Public Announcements**  
**Status of This Notice: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

The Cisco Content Service Switch (CSS) 11000 and 11500 series switches respond to certain Domain Name Service (DNS) name server record requests with an error code and no Start of Authority (SOA) records, which can be negatively cached by some DNS name servers resulting in a potential denial-of-service attack for a particular domain name hosted by a CSS. To be affected by this vulnerability, CSS devices must be configured for Global Server Load Balancing. The CERT/CC issued a vulnerability note on this issue (VU#714121). Cisco is providing repaired software, and customers are urged to upgrade to repaired code.

This vulnerability in CSS is documented as Cisco Bug IDs CSCdz62499 and CSCea36989.

This advisory will be available at <http://www.cisco.com/warp/public/707/cisco-sa-20030430-dns.shtml>.

## Affected Products

The CSS 11000 and 11500 series switches (formerly known as Arrowpoint) consist of the CSS 11050, CSS 11150, CSS 11800 11501, 11503, and 11506 hardware platforms. They run the Cisco WebNS software.

CSS 11000 and 11500 series switches running any WebNS software revision are affected by this vulnerability only if they are configured for Global Server Load Balancing (also known as DNS Load Balancing).

To determine if your CSS equipment is configured for Global Server Load Balancing, please check the configuration for the **dns-server** command. If this command is *not* present, the configuration is not vulnerable to this issue.

No other Cisco product is currently known to be affected by this vulnerability.

## Details

Commonly, the name service in use by the Internet, DNS, uses various record types for queries between DNS servers and clients. The common record types are Address records (A-records), Name Server records (NS records), Mail Exchange (MX records), Start of Authority records (SOA records), and Canonical Name records (CNAME records). Each record or query type has various rules and formats associated with it, including details about what may be cached, what may be trusted by other clients, etc.

Clients usually send queries to a local server, and that local server may send further queries to other servers on behalf of that client in order to formulate a response for the client. When the local server receives the responses, it will cache the information for future use and will respond to the client.

The CSS 11000 and 11500 series switches have the ability to act as an authoritative DNS name server and will only respond to DNS A-record requests. If a CSS configured for DNS via the Global Server Load Balancing feature receives a DNS request or query for an unsupported record type, the CSS will respond with rcode 4 "not implemented" or rcode 3 "NXDOMAIN," depending on the version of WebNS. When an NXDOMAIN response code is received, the querying server will typically stop attempting to resolve any other record type for that name. For example, an NXDOMAIN response to the AAAA query may stop the server from sending an A query, though there may indeed be an A-record in existence. Some resolvers that receive an NXDOMAIN response and support negative caching will not query for A-records for the same name until the negatively cached error response has expired, which can take an extended period of time.

When the DNS query received is for a legitimate host name but an unsupported record type, these negative responses may be cached by various proxies or caching nameservers and will lead to apparent temporary service outages when other clients query the caching nameserver or proxy for the legitimate host name. Though network services are physically unaffected, end users are dependent upon name resolution, and the lack of correct DNS information can result in effective service outages.

Cisco Bug ID CSCdz62499 was the first fix, which changed the response from rcode 3 to rcode 4. This result code is also negatively cached, so the complete fix has been correctly addressed with Cisco Bug ID CSCea36989.

The CSS will now return an RFC 2308-compliant NODATA type 3 response, which is an authoritative answer with rcode=NOERROR, answer=0, and no SOA. This response should cause the specific client to query for another A-record instead of continuing to query for the unsupported record type or using the negatively cached error message or NXDOMAIN answer.

## Impact

Exploitation of this vulnerability would result in a sporadic or partial denial of service, affecting only the users of the DNS services that cache the negative response information in response to an unsupported query type from that same userbase. The administrators of the affected CSS and associated resources may not be aware of any exploitation, since there are no locally apparent symptoms. Only certain user groups would be affected, which may cause significant difficulty in troubleshooting customer reports of problems.

# Software Versions and Fixes

The following table summarizes the CSS software releases affected by the defect described in this notice and provides scheduled dates on which the earliest corresponding fixed releases will be available. Dates are tentative and subject to change.

When selecting a release, keep in mind the following definitions.

- A *maintenance* release is the most heavily tested and highly recommended release.
- An *interim* release has much less testing than a maintenance release and should be selected only if no other suitable release fixes the defect.

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.

Affected Version	Fixed Version	Estimated Date Available
5.00 up to and including 5.00.1.05  • 5.00 build 105 (ap0500105.ad)	5.00.1.08S – Interim Build  • 5.00 build 108s (ap0500108s.ad)	2003–Apr–29
	5.00.2.01 – Maintenance Release  • 5.00 build 201 (ap0500201.ad)	2003–May–30
5.01, 5.02, and 5.03	Upgrade to 6.10 – Maintenance Release	2003–May–15
7.10 up to and including 7.10.1.02  • 7.10 build 102 (sg0710102.ad)	7.20.0.03 – Maintenance Release  • 7.20 build 003 (sg0720002.ad)	Available Now
	7.10.2.06 – Maintenance Release  • 7.10 build 206 (sg0710206.ad)	Available Now

**Note:** Bullet items in the table above provide information on build identifier and file name (previous naming convention for the same build).

## Obtaining Fixed Software

Cisco is offering free software upgrades to remedy this vulnerability for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

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 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 assistance with the upgrade, which should be free of charge.

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). In those cases, customers may only upgrade to a later version of the same release as indicated by the applicable row in the Software Versions and Fixes table. 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)

See <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.

Please 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.

Please do not contact either "[psirt@cisco.com](mailto:psirt@cisco.com)" or "[security-alert@cisco.com](mailto:security-alert@cisco.com)" for software upgrades.

## Workarounds

The workaround for this issue is to disable Global Server Load Balancing and to configure DNS records for the affected servers and domains on a separate compliant DNS server until an upgrade to repaired versions can be installed.

## Exploitation and Public Announcements

This vulnerability has been published by the CERT at <http://www.kb.cert.org/vuls/id/714121>. CERT notes that this issue is not new. The Cisco PSIRT is not aware of any malicious use of the vulnerabilities described in this advisory, but because of the nature of this issue, it may be unlikely that exploitation would be noticed or reported.

## Status of This Notice: FINAL

This is a final notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this notice unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this notice.

## Distribution

This notice will be posted on Cisco's worldwide website at

<http://www.cisco.com/warp/public/707/cisco-sa-20030430-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)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- Various internal Cisco mailing lists

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 1.0	2003-April-30	Initial public release.
Revision 1.1	2003-May-01	Alternate build identifiers added for clarification in Software Versions and Fixes.
Revision 1.2	2003-May-23	Edited Affected Version column contents in the table to clarify version numbers.

## 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](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.

---

Updated: Sep 08, 2004

Document ID: 42486

---