

[NEWS] Cisco Content Service Switch 11000 Series DNS Negative Cache of Information Denial-of-Service Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0004.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/05/03

To: list@securiteam.com

Date: 5 May 2003 18:31:18 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Cisco Content Service Switch 11000 Series DNS Negative Cache of Information Denial-of-Service Vulnerability

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.

DETAILS

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 user base. 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.

A table containing a detailed list of affected products and their corresponding patch can be found at:

<http://www.cisco.com/warp/public/707/cisco-sa-20030430-dns.shtml#software>
<http://www.cisco.com/warp/public/707/cisco-sa-20030430-dns.shtml#software>

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

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" or "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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.