

# Cisco Security Advisory: Cisco Global Site Selector Appliances DNS Vulnerability

Advisory ID: cisco-sa-20090107-gss

<http://www.cisco.com/warp/public/707/cisco-sa-20090107-gss.shtml>

## Revision 1.1

Last Updated 2009 November 12 1400 UTC (GMT)

For Public Release 2009 January 07 1600 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

The Cisco Application Control Engine Global Site Selector (GSS) contains a vulnerability when processing specific Domain Name System (DNS) requests that may lead to a crash of the DNS service on the GSS.

Cisco has released free software updates that address this vulnerability.

A workaround that mitigates this vulnerability is available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090107-gss.shtml>.

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

## ☐ Affected Products

All versions of GSS system software prior to 3.0(1) are affected by this vulnerability. If the GSS is configured with the optional Cisco Network Registrar (CNR) software, the device is not vulnerable.

## ☐ Vulnerable Products

The following GSS products are affected by this vulnerability:

- Cisco GSS 4480 Global Site Selector
- Cisco GSS 4490 Global Site Selector
- Cisco GSS 4491 Global Site Selector
- Cisco GSS 4492R Global Site Selector

In order to determine the software that runs on a GSS device, users should log in to the device and issue the **show version** command to display the system software banner. The version is indicated on the line starting with **Version**. The following example shows a GSS that runs system software 2.0(1):

```
gss.cisco.com#show version

Global Site Selector (GSS)
Model Number: GSS-4491-k9
Copyright (c) 1999-2007 by Cisco Systems, Inc.

Version 2.0(1)

Uptime: 19 Hours 18 Minutes and 14 seconds

gss.cisco.com#
```

In order to determine if CNR is enabled on the GSS device, users should log in to the device and issue the **show running-config | grep cnr** command to display the system CNR configuration. If CNR is enabled, **cnr enable** will be displayed in the output. If CNR is disabled, **no cnr enable** will be displayed. The following example shows a GSS that does not have CNR enabled:

```
GSS.cisco.com#show running-config | grep cnr
no cnr enable
GSS.cisco.com#
```

## ☐ Products Confirmed Not Vulnerable

The following products have been confirmed not vulnerable:

- Cisco Global Site Selector using interaction with Cisco Network Registrar
- Cisco Application Control Engine Module
- Cisco Network Registrar
- Cisco Content Services Switch (CSS)

No other Cisco products are currently known to be affected by this vulnerability.

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

## ▣ Details

The Cisco GSS platform allows customers to leverage global content deployment across multiple distributed and mirrored data locations, optimizing site selection, improving Domain Name System (DNS) responsiveness, and ensuring data center availability.

The GSS is inserted into the traditional DNS hierarchy and is closely integrated with the Cisco CSS, Cisco Content Switching Module (CSM), or third-party server load balancers (SLBs) to monitor the health and load of the SLBs in customers data centers. The GSS uses this information and user-specified routing algorithms to select the best-suited and least-loaded data center in real time.

A vulnerability exists in the GSS when processing a specific sequence of DNS requests. An exploit of the vulnerability may result in a crash of the DNS service on the GSS.

When the DNS server crashes, an error message will appear in the logs similar to the following example:

```
Dec 18 04:47:21 gss NMR-6-LAUNCHSVR_EXIT[27261] dnsserver' has exited [ExitU
```

This vulnerability is documented in Cisco Bug ID: [CSCsj70093](#) ( [registered customers only](#) )

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-3819.

[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>CSCsj70093: GSS DNS service may crash when processing specific DNS requests.</b>					
<b>Calculate the environmental score of <a href="#">CSCsj70093</a></b>					
<b>CVSS Base Score - 7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
<b>CVSS Temporal Score - 6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## ☐ Impact

Successful exploitation of the vulnerability may result in a crash of the GSS DNS service. Repeated exploitation may result in a sustained denial of service (DoS) attack.

[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.

GSS Major Version	First Fixed Release	Recommended Release
1.x(y)	Vulnerable; Option1: Migrate to 3.0(1) or later;	3.0(2)

	Option 2: Migrate to 2.0(5) or later.	
2.x(y)	Vulnerable; Migrate to 2.0(5) or later;	3.0(2)
3.x(y)	Not Vulnerable	

GSS fixed system software is available for download from <http://www.cisco.com/cgi-bin/tablebuild.pl/gss-3des?psrtdcat20e2>

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

## Workarounds

A workaround for this vulnerability requires the administrator to disable the property "ServerConfig.dnsserver.returnError" ( set to zero). On GSS version 1.1(x), 1.2(x) and 1.3(x), this property is disabled by default.

On GSS version 2.0(x), this property is enabled by default (set to one).

The following example shows how to disable this property:

```
GSS#config terminal
GSS(config)#property set ServerConfig.dnsserver.returnError 0
GSS(config)#exit
GSS#write memory
```

To ensure the workaround has been applied properly, from privileged exec mode, execute the **show properties** command and verify that the response returned shows "ServerConfig.dnsserver.returnError" parameter set to zero. The following example shows how to verify the workaround has been successfully applied:

```
gss.cisco.com#show properties | grep ServerConfig.dnsserver.returnError
ServerConfig.dnsserver.returnError : 0
```

For the property to take affect, the GSS should be stopped and restarted:

```
GSS#gss stop
GSS#gss start
```

### Note:

1. GSS version 3.0(x) is not impacted by the issue in the advisory.
2. GSS version 1.x(y) is not impacted by the issue in the advisory so long as the negative return property has not been changed from its default settings. [GSS versions 1.1(x), 1.2(x) and 1.3(x) ship with this property disabled. GSS version 1.0(x) does not allow user customization of the property command].
3. GSS version 2.0.x is vulnerable. [GSS version 2.0.x ships with this property enabled].

### Mechanics of the Workaround

If there is a query for which there is no domain match on the GSS, such a query is dropped and the DNSQueriesUnmatched counter is incremented. As a side-effect of the workaround, neither of the negative responses NXDOMAIN,NODATA are sent for queries for which there is no domain match.

### **Impact of the Workaround**

1. If there are no Authority Domains configured on the GSS, there is no impact that will be noticed by the end-user.
2. If there are Authority Domains configured on the GSS, and since disabling negative response will result in no communication to the resolver, the resolver receives no indication whether the lack of response is because of network failure or because that domain was not supported by the GSS. This lack of knowledge will result in the resolver attempting to send the same query for a domain that does not exist on the GSS again if it receives a request for such a domain from a DNS client.

[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 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 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

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/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) 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 aware of active exploitations where malicious use of the vulnerability described in this advisory has occurred.

This vulnerability was discovered by investigating customer TAC service requests.

[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-20090107-gss.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-bulletins@lists.first.org](mailto:first-bulletins@lists.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 1.1	2009-November-12	Updated workarounds
Revision 1.0	2009-January-07	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)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

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