

# Cisco Security Advisory: Cisco Guard Enables Cross Site Scripting

Document ID: 71506

Advisory ID: cisco-sa-20060920-guardxss

<http://www.cisco.com/warp/public/707/cisco-sa-20060920-guardxss.shtml>

## Revision 1.0

For Public Release 2006 September 20 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

[Summary](#)  
[Affected Products](#)  
[Details](#)  
[Impact](#)  
[Software Version and Fixes](#)  
[Workarounds](#)  
[Obtaining Fixed Software](#)  
[Exploitation and Public Announcements](#)  
[Status of this Notice: FINAL](#)  
[Distribution](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Summary

A vulnerability in the Cisco Guard may enable an attacker to send a web browser client to a malicious website with the use of Cross Site Scripting (XSS) when the Guard is providing anti-spoofing services between the web browser client and a webserver. The attacker may exploit this by providing a malicious URL for the web browser client to go to, often in email, followed off of a malicious website, or in an instant message. This issue may occur even if the protected website does not allow XSS. A software upgrade is required to fix this vulnerability. There is a workaround available to mitigate the effects of the vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20060920-guardxss.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

The following Cisco products are vulnerable.

- Cisco Guard Appliance (Software Version 3.X)
- Cisco Guard Blade (Software Version 4.X)
- Cisco Guard Appliance [Software Version 5.0(3)]
- Cisco Guard Appliance [Software Version 5.1(5)]

## Products Confirmed Not Vulnerable

No other Cisco products have been found to be vulnerable.

There are three ways to determine the software version that your Cisco Guard DDoS mitigation appliance is running. An example of each method is shown here:

- **Virtual terminal or local serial console connection**

To determine the software version number through the local serial console use a serial cable and a terminal emulation program to connect to the appliance. Once you are connected, press the **Enter** key of your terminal and the Guard will present, without even logging in, the version of the software running on the devices:

```
Cisco Guard Version 3.1(0.12)
```

```
GUARD login:
```

In this example the Cisco Guard is running software version 3.1.

For a virtual terminal, the procedure is the same except that no serial cable or terminal emulation program is needed (a standard keyboard and monitor are directly connected to the appliance).

- **Remote Secure Shell (SSH) connection**

To obtain the software version number through a SSH session, use a SSH client to log in to the Cisco Guard and issue the **show version** command—line interface (CLI) command.

```
prompt$ ssh admin@guard.example.com
admin@guard.example.com's password:
Last login: Wed Nov 24 22:45:53 on ttyS0
admin@GUARD#show version
Copyright (c) 2000-2004 Cisco Systems, Inc. All rights reserved.
```

```
Software License Agreement
```

```
[...]
```

```
Cisco Anomaly Guard
Release: 3.1(0.12)
Date:    2004/10/27 19:58:14
```

```
GUARD uptime is 3 weeks, 3 days, 17 hours, 53 minutes
System Serial Number: XXXXXXXX
```

In this example, the Cisco Traffic Anomaly Guard is running software version 3.1.

- **Remote secure web session**

To obtain the software version that Cisco Guard is running through a secure web interface, open the URL **https://IP address of your Guard/** in a web browser, log in, and then click on the **About** link located on the top right section of the browser window.

## Details

The Cisco Guard DDoS Mitigation Appliance is a distributed denial-of-service (DDoS) protection system. Malicious DOS traffic is identified with a Cisco Detector and diverted to the Guard for attack mitigation. Under normal circumstances, the Guard plays no role in valid traffic; it is specifically designed to deal with large volumes of invalid traffic.

Cross Site Scripting (XSS) is an attack where a user follows a link that contains an embedded script. The link often looks valid, and sends the user to a valid site. The recipient website does not contain the link that is sent and sends a meta-refresh back to the user without validating the data it is sent. When receiving the meta-refresh, the web browser interprets the script as an instruction from the website and the script is executed on the user's machine .

In this case, when the anti-spoofing feature is enabled, all diverted HTTP traffic is inspected and then a meta-refresh is sent to the client containing the original request. If the original URL contains a script and a specific character sequence, the meta-refresh from the Guard will allow the client machine to execute the malicious script.

Several conditions are required to be true in order for the malicious script to be processed:

- The client user must follow a URL with a specifically formatted, embedded script to a site protected by the Guard.
- The Guard must be running active basic protection, going through basic/redirect protection.
- The specially crafted http request must be diverted through the Guard, and processed by the Guard.

Only if all of the above conditions are met will the client receive the meta-refresh and process the embedded script.

This vulnerability is being tracked by bug ID CSCsf01438 ( registered customers only) .

## Impact

Successful exploitation of the vulnerability may result in malicious executable code being run by an individual user using a web browser.

## Software Version and Fixes

This vulnerability is fixed in version 5.1(6) of the Cisco Anomaly Guard code.

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.

## Workarounds

Changing the basic/redirect protection to basic/safe-reset protects the client from executing the embedded script. Instead of providing a layer seven http meta-refresh to the browser with the malicious URL intact, the Guard provides a layer three TCP-RST to end the connection. This can cause minor compatibility issues, as some firewalls do not forward the TCP-RST. However, this method protects users from any XSS attacks until

Cisco Security Advisory: Cisco Guard Enables Cross Site Scripting

the Guard can be upgraded to a fixed version of code.

To turn off basic/redirect and configure basic/safe-reset, please follow the example below.

1. Show the zone.

```
user@GUARD#show zone test

...skipped

**** USER FILTERS ****
Row Source IP Source Mask      Proto DPort Frg Action Rate Burst Units RxRate(pps)
10 *          255.255.255.255 6      80    no  basic/redirect

user@GUARD#config t
user@GUARD-conf#zone test
user@GUARD-conf-zone-test#no user-filter 10
```

2. Configure basic/safe-reset dynamic filter.

```
user@GUARD-conf-zone-test#user-filter 10 basic/safe-reset * 6 80
```

3. Show that the filter is applied.

```
user@GUARD#show zone test

...skipped

**** USER FILTERS ****
Row Source IP Source Mask      Proto DPort Frg Action Rate Burst Units RxRate(pps)
10 *          255.255.255.255 6      80    no  basic/safe-reset
```

For more information, please refer to the configuration guide:

[http://www.cisco.com/en/US/products/ps5888/products\\_configuration\\_guide\\_chapter09186a00804b7d13.html#wp113](http://www.cisco.com/en/US/products/ps5888/products_configuration_guide_chapter09186a00804b7d13.html#wp113)

## Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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/cgi-bin/tablebuild.pl/cisco-ga-crypto?psrtdcat20e2> ( registered customers only) for the appliance or <http://www.cisco.com/cgi-bin/tablebuild.pl/cisco-agm-crypto?psrtdcat20e2> ( registered customers only) for the 7600 module.

# 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](mailto: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.

This vulnerability was reported to Cisco by a customer.

## 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 is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20060920-guardxss.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.

## Revision History

Revision 1.0	<del>2006 September 20</del>	<del>Initial public release.</del>
--------------	------------------------------	------------------------------------

## 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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Sep 20, 2006

Document ID: 71506

---