FORTCONSULT

Straight talk on IT security

SECURITY ADVISORY

December 2008

Barracuda Load Balancer admin login Cross-site Scripting

Discovered in December 2008 by FortConsult's Security Research Team/Jan Skovgren

WARNING – NOT FOR DISCLOSURE BEFORE PUBLIC RELEASE

This document contains proprietary and confidential information. An informal and nonbinding understanding exists between Barracuda Networks and FortConsult that, for the safety of our customers and other users, the details of this advisory will not be made public until February 2009. Please DO NOT forward this document to ANYONE, in any way whatsoever.

Table of Contents

Copyright and Disclaimer

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team/Jan Skovgren

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: www.fortconsult.net.

FortConsult
Tranevej 16-18
DK-2400 Copenhagen NV
Tel +45 7020 7525
Fax +45 7020 7526
www.fortconsult.net

Issue History

This document has been updated to the present version as information has been received from various external sources.

9th. December 2008: Issue discovered by Jan Skovgren
9th. December 2008: Vendor was contacted
10th. December 2008: Vendor reports back
15th. December 2008: Vendor issues a fix Link
5th. February 2009: Disclosure date Link

THIS DOCUMENT IS TENTATIVELY SCHEDULED FOR PUBLIC RELEASE VIA THE FORTCONSULT WEBSITE AND SECURITY MAILING LISTS IN February 2009.

Issue Description

The administrative application used for login to the Barracuda Load balancer is vulnerable to cross-site scripting. Cross-site scripting vulnerabilities occur when a web application uses client-supplied data in an HTTP response without first filtering out potentially malicious characters.

To carry out a cross-site scripting attack, an attacker will create a URL that takes advantage of a cross-site scripting flaw. The attacker must then find some way of getting a victim to visit this URL. This can be done in many ways, ranging from getting it listed in a search engine to exploiting weaknesses in mail clients that allow scripted content to be executed. Once the victim has used the cross-site scripting URL, the attacker's malicious code will be executed on his or her system. A common goal of these attacks is to capture the victim's cookie. A cookie is an authentication token that a webserver uses to determine the identity of a client. With a victim's cookie, an attacker can launch a session hijacking attack and gain access to the victim's account or other personal information on the webserver.

Issue Impact

This makes the site easier to "phish" and can be used to attack the site's clients when they connect to the site. It can make it possible for an attacker to steal information from the client machines that connect to the site.

Affected Components

Barracuda Load Balancer 640
Maybe other Barracuda products with web admin interface.

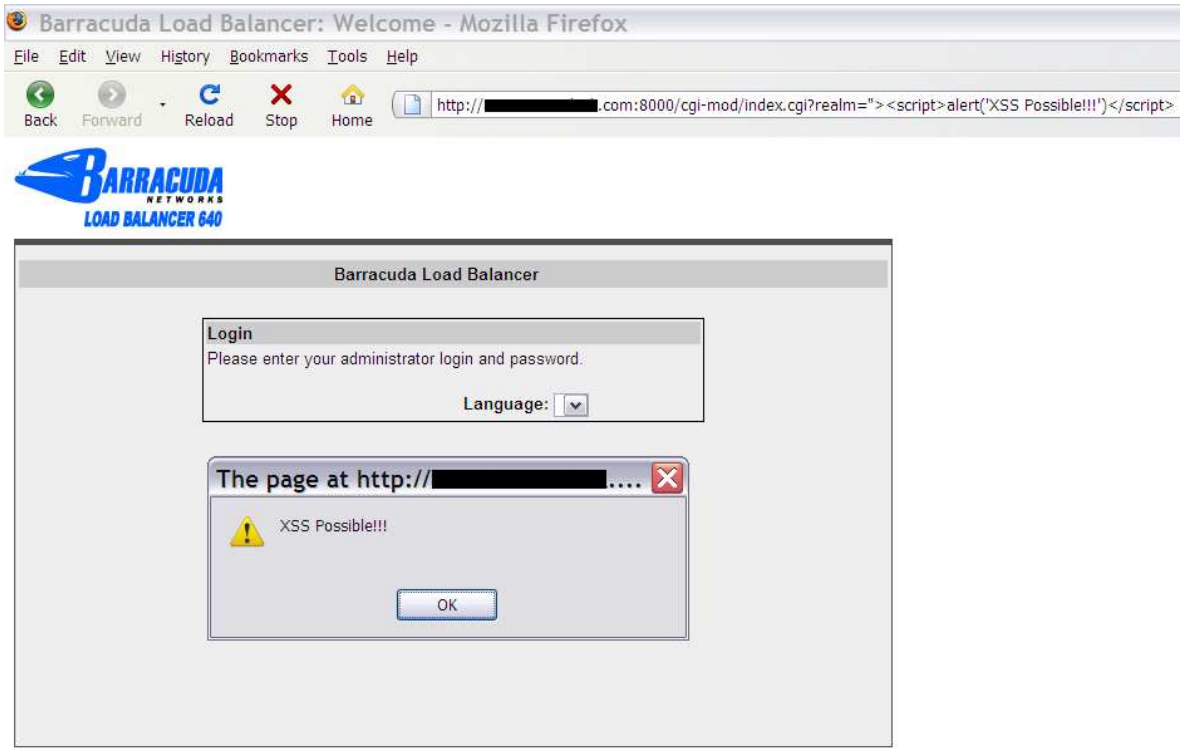
FortConsult
Tranevej 16-18
DK-2400 Copenhagen NV
Tel +45 7020 7525
Fax +45 7020 7526
www.fortconsult.net

Exploit

It is the “realm” parameter that is vulnerable to cross-site scripting.
Navigate your web browser to:

http://vulnerablesite/cgi-mod/index.cgi?realm="><script>alert(‘XSS Possible!!!’)</script>

This will execute the injected javascript code “<script>alert(‘XSS Possible!!!’)</script>” and produce an alertbox with the text “XSS Possilbe!!!” which proofs that the “realm” parameter is vulnerable to Cross-site scripting. See screen dump below.



Tested on FireFox 3.0.4 and IE 7.0.5730.13

Mitigation

As a temporary workaround whilst on standby for the vendor to release a fix or an updated version you may want to attempt own input validation at the Firewall Layer, if this is possible. You could also use some other custom-made input validation solution.

CVE-reference

None yet.

FortConsult
Tranevej 16-18
DK-2400 Copenhagen NV
Tel +45 7020 7525
Fax +45 7020 7526
www.fortconsult.net

CVSS Base Score

FortConsult has used the online CVSS calculator found at http://nvd.nist.gov/cvss.cfm?calculator&version=2 to calculate these scores.

BASE SCORE: 4.3

Metrics:

Access Vector: Network

Access Complexity: Medium

Authentication: None

Confidentiality Impact: None

Integrity Impact: Partial

Availability Impact: None

FortConsult
Tranevej 16-18
DK-2400 Copenhagen NV
Tel +45 7020 7525
Fax +45 7020 7526
www.fortconsult.net