NNL-Labs & MNIN | F5 FirePass Security Advisory

January 05, 2007

Summary

This document describes multiple XSS, filter bypass, and information disclosure vulnerabilities in F5 FirePass SSL VPN. Additional interesting vulnerabilities on this product may be released in the future depending on various other circumstances.

Vendor description: http://f5.com/products/FirePass

"F5's FirePass® SSL VPN appliance provides secure access to corporate applications and data using a standard web browser. Delivering outstanding performance, scalability, ease-of-use, and end-point security, FirePass helps increase the productivity of those working from home or on the road while keeping corporate data secure."

Affected Versions

For reasons withheld, this advisory will not contain details on vulnerable versions of FirePass. However, this information should certainly be available from the vendor's website. We would suggest creating a portal account and viewing the F5 CERT advisories and vulnerabilities page. Hotfixes may be available for some of the affected versions.

Credit and Contact

Michael Ligh from (http://mnin.org) and Greg Sinclair (security@nnlsoftware.com)

Event Timeline

Jul 2006	Discovered and reported a majority of vulnerabilities
…	Long story, don't ask.
Nov 2006	Reported additional filter bypass vulnerabilities
Nov 2006	F5 vulnerability response policy updated/modified
Dec 2006	Reported additional filter bypass vulnerabilities
Dec 2006	Reported additional filter bypass vulnerabilities
Dec 2006	F5 publishes one of the vulnerabilities: #1
Jan 2007	24-hour notice of publishing this document given to F5
Jan 2007	F5 publishes three more vulnerabilities: #2, #3, #4
Jan 2007	This document disclosed to public
Jan 2007	F5 publishes two more vulnerabilities: #5, #6

Details

XSS vulnerability on main FirePass logon page (xcho)

A cross-site scripting vulnerability was identified in the main logon page, my.logon.php3. The URL contains two key parameters: crs and xcho. The xcho parameter is a Rot13 encoded message that is displayed in the logout page and the crs parameter is a CRC32 hash value. If the value of the crs parameter does not match the CRC32 of the decoded xcho value, then the message is not displayed. However, if the hash value does match, the user-supplied xcho parameter is decoded and displayed in the page. An attacker simply needs to Rot13 encode the script to be executed, compute the CRC32 value, and send the resulting URL to a logged-in user.

Multiple XSS vulnerabilities within administration console

The system's Global Customization page (/vdesk/admincon/index.php?a=per) does not properly filter input for Custom colors (topblue, midblue, wtopblue, etc.) or Front Door custom text colors (h321, h311, h312, etc.) values.

The New Browsers page (/vdesk/admincon/index.php?a=bro) does not properly filter input for the User Agent (ua) value.

The Launch Applications page (/vdesk/admincon/webyfiers.php) does not properly filter input for the App Path (app_name) and Parameters (app_param) values.

These findings are contained within the FirePass administration module. Scripts injected via these values are persistent on the page and will repeatedly execute in an administrator's browser until manually removed.

XSS with double eval() Javascript and FP_DO_NOT_TOUCH tags

By calling JavaScript that performs a double eval(), arbitrary JavaScript could be executed in the client's browser in a reverse-proxy scenario. Eval() functions are re-written by the FirePass engine, but double eval() functions are ignored. Any JavaScript within <FP_DO_NOT_TOUCH> tags is also ignored, bypassing the anti-XSS mechanism implemented by the FirePass.

XSS vulnerability on main FirePass activation page (vhost)

An XSS vulnerability has been identified in the vhost parameter of the my.activation.php3 logon page.

LDAP authentication information leak

An information disclosure vulnerability was identified in the activation page - my.activation.php3. When a user attempts to login to the system but fails to provide proper credentials, the system will return the error message "*Either Username or Password do not match! Please try again.*" If the username provided exists in the LDAP (i.e., the user is authorized to access the FirePass), the message will display the word "*password*" in lowercase. However, if the username provided does not exist in the LDAP, the word "*Password*" is displayed in the error message in uppercase.

ACL Filter bypass with URL de-normalization

FirePass either applies its blacklist filtering rules before URL canonicalization, or its canonicalization routines are simply not sufficient. Therefore, one can bypass filters and access restricted URLs by using one or more of the following techniques (assuming the blacklist "Deny" filter exists for "site.com/path/file.html").

a) place a trailing NULL byte after the requested URL (e.g. /path/file.html%00)
b) place two or more slashes in the URL (e.g. //path/file.html)
c) encode all or part of the request in Unicode (e.g. /path/%66%69%6C%65.html)
d) use simple directory traversal techniques (e.g. /blah/%2e%2e/path/file.html)
e) use even more simple directory techniques (e.g. /%2e/path/file.html)
f) capitalize a letter in the domain (e.g. site.coM/path/file.html)

Filter bypass with dword-encoded IP address

Authenticated users can easily evade host access restrictions by converting the destination server's IP address to a dword-encoded format and sending the resulting URL via the FirePass URL encoding mechanism. Among other possibilities, this vulnerability allows remote users to access the FirePass administrator console if the requested URL is a dword-encoded form of the FirePass' own localhost address. For example, after logging into the FirePass as a normal end-user, requesing "http://site.com/vdesk/admincon" or "http://127.0.0.1/vdesk/admincon" will be blocked, however requesting

"http://16909060/vdesk/admincon" will grant access to the console (attacker must still authenticate).

Attributions

The image of a 5-year old writing 2+2=5 on a chalk board was purchased from istockphoto.com for one dollar.

License