



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**July 23, 2009**

*The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**ADVISORY NUMBER:**

SA2009-036

**DATE(S) ISSUED:**

7/23/2009

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Firefox Could Allow Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Mozilla Firefox, a popular web browser used to access the Internet. These vulnerabilities could allow attackers to execute arbitrary code on affected systems. These vulnerabilities may be exploited if a user visits a specifically crafted web page, or opens a specially crafted file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user account, an attacker could then install programs; view, change, or delete data; or create new accounts with user level of logged on user. Failed exploit attempts may result in a denial-of-service condition.

**Please note that these are new vulnerabilities which were not mitigated by the patch that was issued earlier this week as described in our July 21, 2009 Advisory 2009-042.**

**SYSTEMS AFFECTED:**

- Mozilla Firefox 3.0, Beta 5
- Mozilla Firefox 3.0.1
- Mozilla Firefox 3.0.2
- Mozilla Firefox 3.0.3
- Mozilla Firefox 3.0.4
- Mozilla Firefox 3.0.5
- Mozilla Firefox 3.0.6
- Mozilla Firefox 3.0.7
- Mozilla Firefox 3.0.8
- Mozilla Firefox 3.0.9
- Mozilla Firefox 3.0.10
- Mozilla Firefox 3.0.11
- Mozilla Firefox 3.5

- Mozilla Thunderbird 1.5.0 - 2.0.8

## **RISK:**

### **Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

### **Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

### **Home users: High**

## **DESCRIPTION:**

Mozilla FireFox is a web browser that allows a user to view web page content. Multiple vulnerabilities have been discovered in Mozilla Firefox that could allow an attacker to take complete control of an affected system.

### **Multiple Firefox Remote Memory Corruption Vulnerabilities**

Four vulnerabilities exist as a result of multiple memory-corruption errors that are contained in the browser engine. The first issue is an integer overflow in a base64 decoding function. The second vulnerability exists in the way that Firefox handles RDF (Resource Description Framework) files in the XUL tree. XUL (XML User Interface Language) is Mozilla's XML-based language that lets a developer build applications. Two additional vulnerabilities exist in the Mozilla JavaScript engine where a document can be created whose internal representation contains duplicate elements leading to potentially unsafe memory conditions.

### **Firefox 'setTimeout' Remote Code Execution Vulnerability**

Mozilla Firefox is prone to a vulnerability due to an error when 'setTimeout()' is invoked with certain object parameters defined. Successful exploitation could result in the execution of arbitrary Javascript code with chrome privileges. Mozilla Chrome is the user interface parts of the application window that are outside of a window's content area. Toolbars, menu bars, progress bars, and window title bars are all examples of elements that are typically part of the chrome.

### **Firefox Flash Player Remote Code Execution Vulnerability**

A vulnerability exists when navigating to another web page that contains a Flash object which presents a slow script dialog. While the dialog is still visible to the user, the Flash plugin is unloaded, resulting in a crash due to a call to the deleted object.

### **Firefox Remote Code Execution Vulnerability**

Remote code can be executed as a result of the way in which Firefox handles the 'watch' and 'defineSetter' functions for SVG elements. SVG (Scalable Vector Graphics) is an XML language for sophisticated 2D graphics.

### **Firefox Overflow Vulnerabilities**

A series of heap and integer overflow vulnerabilities exist which independently affected multiple font glyph rendering libraries. These overflow issues impact Macintosh OS X's CoreGraphics package, as well as Linux's Libpango package. No Microsoft graphics packages were shown to be affected by these vulnerabilities.

Successful exploitation of any of the vulnerabilities identified above could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user account, an attacker could then install programs; view, change, or delete data; or create new accounts with user level of logged on user. Failed exploit attempts may result in a denial-of-service condition.

#### **Firefox Cross-origin Wrapper Bypass Vulnerability**

A vulnerability exists in the way that Firefox constructs the 'XPCCrossOriginWrapper' which may result in cross-site scripting attacks. Successful exploitation could result in an attacker gaining access to another site's JavaScript content. This could then be used to create XSS attacks and run JavaScript within the context of another site.

**Please note that these are new vulnerabilities which were not mitigated by the patch that was issued earlier this week as described in our July 21, 2009 Advisory 2009-042.**

#### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Install the appropriate vendor patches and upgrades immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

#### **REFERENCES:**

##### **Secunia:**

<http://secunia.com/advisories/35914/>

##### **Security Focus:**

<http://www.securityfocus.com/bid/35765/>

<http://www.securityfocus.com/bid/35766/>

<http://www.securityfocus.com/bid/35767/>

<http://www.securityfocus.com/bid/35769/>

<http://www.securityfocus.com/bid/35770/>

<http://www.securityfocus.com/bid/35772/>

<http://www.securityfocus.com/bid/35773/>

<http://www.securityfocus.com/bid/35774/>

<http://www.securityfocus.com/bid/35775/>

<http://www.securityfocus.com/bid/35776/>

##### **Mozilla:**

<http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>

<http://www.mozilla.org/security/announce/2009/mfsa2009-35.html>

<http://www.mozilla.org/security/announce/2009/mfsa2009-36.html>

<http://www.mozilla.org/security/announce/2009/mfsa2009-37.html>

<http://www.mozilla.org/security/announce/2009/mfsa2009-39.html>  
<http://www.mozilla.org/security/announce/2009/mfsa2009-40.html>  
<https://developer.mozilla.org/en/Chrome>  
<https://developer.mozilla.org/en/XUL>  
<http://www.mozilla.org/projects/svg/>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1194>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2462>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2463>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2464>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2465>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2466>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2467>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2468>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2469>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2471>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2472>