



State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory

August 4, 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:**  
SA2009-042

**DATE(S) ISSUED:**  
8/4/2009

**SUBJECT:**  
Multiple Vulnerabilities in Mozilla Products

**OVERVIEW:**  
Multiple vulnerabilities have been discovered in Mozilla applications. Mozilla provides various Internet applications such as web browsers (Firefox), email clients, and web development tools. 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 of four of these vulnerabilities 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 full user rights. Failed exploit attempts may result in a denial-of-service condition.

**SYSTEMS AFFECTED:**

- Mozilla Firefox 3.5.1 and earlier
- Mozilla Firefox 3.0.12 and earlier
- Mozilla Thunderbird 2.0.0.22 and earlier
- Mozilla SeaMonkey 1.1.17 and earlier
- Mozilla Network Security Services (NSS) 3.12.2 and earlier

**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:**

Multiple vulnerabilities have been discovered in the Mozilla Firefox, SeaMonkey, and Thunderbird applications which could allow for remote code execution or by-pass security policies. The Mozilla Firefox and Thunderbird applications are used to browse the web, and handle email respectively. SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Network Security Services (NSS) is a set of libraries designed to support development of security-enabled client and server applications.

#### **Mozilla Firefox Error Page Address Bar URI Spoofing Vulnerability**

A vulnerability exists when navigating away from a malicious web page. Specifically, a 'window.open()' call with a URI containing an invalid character will trigger an error page, but the URI displayed in the address bar will look legitimate. This could mis-lead the user in to clicking on links on the page thinking they are legitimate which may lead to additional attacks.

#### **Mozilla Firefox Incorrect Security Wrapper JavaScript Chrome Privilege Escalation Vulnerability**

Mozilla Firefox is prone to a privilege escalation vulnerability due to an incorrect security wrapper passed to the 'window' global object. This issue occurs when an add-on implementing a Content Policy opens pages that have the 'Link:' HTTP header. Successful exploitation could result in the execution of arbitrary JavaScript code with Chrome Privileges. Mozilla Chrome is the area of the application window that are outside of the content area. Toolbars, menu bars, progress bars, and window title bars are all examples of elements that are typically part of Chrome.

#### **Mozilla Firefox Multiple Memory Corruption Vulnerabilities**

Multiple vulnerabilities exist as a result of multiple memory-corruption errors. The first issues involve 'vorbis\_book\_decodevv\_add' at vorbis\_codebook.c' and the 'jstracer.cpp' source files of the 3.5.x versions of Firefox. Another issue involves the 'jsdbgapi.c' source file of the 3.0.x versions of Firefox. 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 full user rights. Failed exploit attempts may result in a denial-of-service condition.

#### **Mozilla Firefox SOCKS5 Proxy Response Denial of Service Vulnerability**

A vulnerability exists as a result of a memory-corruption error. This error occurs because SOCKS5 proxy replies containing a DNS name longer than 15 characters may corrupt subsequent data streams in proxy responses. There is a possibility that remote code execution can occur but has not been confirmed at this time. Successful exploitation of the vulnerability 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 full user rights. Failed exploit attempts may result in a denial-of-service condition.

#### **Mozilla Products NULL Character CA SSL Certificate Validation Security Bypass Vulnerability**

Mozilla products are prone to a security-bypass vulnerability. The applications fail to properly validate the domain name in a signed CA certificate. The applications stop reading the domain name when it encounters a NULL character. Such an alleged subdomain may look like 'example1.com\0example.com' where the attacker owns 'example.com' and wishes to impersonate 'example1.com'. Successful exploitation will allow attackers to perform man-in-the-middle attacks or impersonate trusted servers.

### **Mozilla Firefox and Seamonkey Regular Expression Parsing Heap Buffer Overflow Vulnerability**

The applications are prone to a heap-based buffer-overflow vulnerability. This vulnerability involves the regular expression parser and how it is used to match common names in SSL certificates. Note that attackers need to exploit this issue with a crafted certificate that the application trusts; otherwise, a warning message will be presented to the user. Successful exploitation of the vulnerability 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 full user rights. Failed exploit attempts may result in a denial-of-service condition.

### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply the appropriate update to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Ensure that all anti-virus software is up to date with the latest signatures.

### **REFERENCES:**

#### **Security Focus:**

<http://www.securityfocus.com/advisories/17503>

<http://www.securityfocus.com/advisories/17504>

<http://www.securityfocus.com/advisories/17505>

<http://www.securityfocus.com/advisories/17509>

<http://www.securityfocus.com/advisories/17535>

<http://www.securityfocus.com/archive/1/145a3a30907270523i3a5b38acm214b744346c813ee@mail.gmail.com>

<http://www.securityfocus.com/archive/1/200907242046.n6OKkXI6018771@www3.securityfocus.com>

<http://www.securityfocus.com/archive/1/20090727134451.11982.qmail@securityfocus.com>

#### **Mozilla:**

<http://www.mozilla.org/security/announce/2009/mfsa2009-44.html>

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=498897](https://bugzilla.mozilla.org/show_bug.cgi?id=498897)

<http://www.mozilla.org/security/announce/2009/mfsa2009-46.html>

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=502832](https://bugzilla.mozilla.org/show_bug.cgi?id=502832)

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=501270](https://bugzilla.mozilla.org/show_bug.cgi?id=501270)

[https://bugzilla.mozilla.org/show\\_bug.cgi?id=500254](https://bugzilla.mozilla.org/show_bug.cgi?id=500254)

<http://www.mozilla.org/security/announce/2009/mfsa2009-45.html>  
<http://www.mozilla.org/security/announce/2009/mfsa2009-38.html>  
<http://www.mozilla.org/security/announce/2009/mfsa2009-42.html>  
<http://www.mozilla.org/security/announce/2009/mfsa2009-43.html>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2654>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2470>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2408>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2404>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2409>