



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

July 14, 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:

SA2009-034

DATE(S) ISSUED:

7/14/2009

7/17/2009 – UPDATED

SUBJECT:

Vulnerability in Mozilla Firefox Could Allow Remote Code Execution

OVERVIEW:

A new vulnerability has been discovered in the Mozilla Firefox which could allow attackers to execute arbitrary code on affected systems. Mozilla Firefox is a web browser used to access the Internet. Exploitation can occur if a user visits a webpage designed to take advantage of this vulnerability. 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 full user rights. Failed exploit attempts may result in a denial-of-service condition.

There is no patch available at this time.

SYSTEMS AFFECTED:

- Mozilla Firefox 3.5

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:

A vulnerability has been discovered in the way the Mozilla Firefox web browser handles specific escaped characters while processing them in its JavaScript environment. When processing JavaScript, certain string characters are escaped and loaded into the buffer. This vulnerability may be exploited if a user visits a maliciously crafted web page. Successful exploitation could result in an attacker gaining user level privileges. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

We have confirmed in our lab that exploitation of this vulnerability in Firefox 3.5 on both Windows XP SP2 and SP3 can result in remote code execution.

UPDATE – 7-17-2009:

The Mozilla Foundation has released Firefox 3.5.1 to address a vulnerability. This vulnerability is due to an error in the way the Just-in-Time (JIT) compiler returns from native functions.

Exploitation of this vulnerability may allow an attacker to execute arbitrary code.

US-CERT encourages users and administrators to review Mozilla Foundation Security Advisory 2009-41 and upgrade to Firefox 3.5.1 or apply the suggested workaround provided in the advisory. Additional information can also be found in the Vulnerability Notes Database.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Install the appropriate vendor patch as soon as it becomes available 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/35798/2/>

Security Focus:

<http://www.securityfocus.com/bid/35660>