



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

March 31, 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:

SA2009-019

DATE(S) ISSUED:

3/27/2009

SUBJECT:

Vulnerability in Mozilla Firefox Could Allow for Remote Code Execution

OVERVIEW:

A new vulnerability has been discovered in the Mozilla Firefox web browser 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 specifically crafted 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.

We have confirmed that Firefox 3.0.7 crashes with the proof-of-concept code that is publicly available. Mozilla will be releasing a fix for this vulnerability via the 3.0.8 release. This fix is expected to be available sometime during the week of 3/30/2009.

SYSTEMS AFFECTED:

- Mozilla Firefox 3.0
- 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

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 new vulnerability has been discovered in the Mozilla Firefox web browser. The vulnerability involves processing of malformed XML files. Specifically, Firefox fails to properly handle specially crafted 'root' tags contained in an XML file. A 'root' tag is the first element defined in an XML file. All other tags are nested within the root tag.

The vulnerability can be exploited by an attacker if a user visits a specially crafted malicious web site. Successful exploitation could result in an attacker gaining the same privileges as the logged on user within the context of the affected browser. 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.

We have confirmed that Firefox 3.0.7 crashes with the proof-of-concept code that is publicly available. Mozilla will be releasing a fix for this vulnerability via the 3.0.8 release. This fix is expected to be available sometime during the week of 3/30/2009.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Mozilla, as soon as they are available, after appropriate testing.
- Do not 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.
- Do not download or open files from un-trusted websites.

REFERENCES:

Mozilla Security Blog:

<http://blog.mozilla.com/security/2009/03/26/cansecwest-2009-pwn2own-exploit-and-xsl-transform-vulnerability/>

SANS:

<http://isc.sans.org/diary.html?storyid=6079>

Security Focus:

<http://www.securityfocus.com/bid/34235>

Network World:

<http://www.networkworld.com/news/2009/032609-firefox-fix-due-next-week.html>

ZDNet:

<http://blogs.zdnet.com/security/?p=3013>