



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

December 18, 2008

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.

STATE OF ALASKA ADVISORY NUMBER:

2008-031

DATE(S) ISSUED:

12/18/2008

SUBJECT:

Vulnerabilities in Mozilla Firefox could allow remote execution of malicious code

OVERVIEW:

Mozilla developers identified and fixed several stability bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these crashes showed evidence of memory corruption under certain circumstances and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

SYSTEMS AFFECTED:

- Mozilla Firefox v. 2 & 3
- Thunderbird
- Seamonkey

RISK:

Government:

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

Businesses:

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

Home users: High

DESCRIPTION:

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to bypass certain security restrictions, disclose sensitive information, conduct cross-site scripting attacks, or potentially compromise a user's system.

1. Errors in the layout and JavaScript engines can be exploited to corrupt memory and potentially execute arbitrary code.
2. An error when processing the "persist" XUL attribute can be exploited to bypass cookie settings and uniquely identify a user in subsequent browsing sessions.
3. Multiple errors can be exploited to bypass the same-origin policy, disclose sensitive information, and execute JavaScript code with chrome privileges.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Mozilla/Firefox to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Read all e-mail messages in plain text.

REFERENCES:**Mozilla:**

<http://www.mozilla.org/security/announce/2008/mfsa2008-60.html>

CRN:

<http://www.crn.com/security/212501064>