

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE (S) ISSUED:

4/22/2015

SUBJECT:

Vulnerability in Mozilla Firefox Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been identified in Mozilla Firefox, which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet. Successful exploitation may allow an attacker to execute arbitrary code in the context of the user running the affected application or result in denial-of-service conditions. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

Mozilla Firefox versions prior to 37.0.2

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

TECHNICAL SUMMARY:

A use-after-free, memory-corruption vulnerability has been reported in Mozilla Firefox. This vulnerability exists due to a race condition that occurs when the application fails to properly initialize a plugin.

Specifically, this issue occurs due to a crash in the 'AsyncPaintWaitEvent::AsyncPaintWaitEvent(nsIContent*, bool)' function.

This vulnerability can be exploited if a user visits, or is redirected to, a specially crafted web page using the affected program. Successful exploitation of this vulnerability could result in remote code execution, allowing an attacker to run code in the context of the user running the affected application.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade to latest versions of Mozilla Firefox after appropriate testing.

Run all software as a non-privileged user to diminish effects of a successful attack.

Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-45/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2706>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>