

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 ISSUED:

08/07/2015

SUBJECT:

Vulnerability in Mozilla Firefox Could Allow for Privilege Escalation

OVERVIEW:

A vulnerability has been identified in Mozilla Firefox which could allow for Privilege Escalation. Mozilla Firefox is a web browser used to access the Internet. Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of this vulnerability may result in an attacker being able to read and steal sensitive local files on the victim's computer.

THREAT INTELLIGENCE:

Mozilla has received information that indicates an exploit for this vulnerability has been found in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 39.0.3
- Firefox ESR versions prior to 38.1.1

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 vulnerability has been discovered in Mozilla Firefox's built-in PDF viewer that may allow an attacker to view and steal sensitive files on a victim's computer. This exploit occurs by injecting a JavaScript payload into the local file context, which allows the script to search for and upload potentially sensitive local files of the user. This vulnerability can be exploited in the background when a user visits a specially crafted webpage with the exploit code embedded. The exploit specifically looks for FTP configuration files, subversion, s3browser, Filezilla, libpurple and other account information on a Windows system and Global configuration files and user directories on a Linux system.

Note: Mac users are not susceptible to the currently available exploit code, however the underlying vulnerability still exists within Mozilla Firefox for Macs and could be exploited by an attacker by creating a different payload.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates 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.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-78>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4495>

The Hacker News:

<http://thehackernews.com/2015/08/mozilla-firefox-update-download.html>

TLP: WHITE

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

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