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:
12/08/2015

SUBJECT:
Cumulative Security Update for Internet Explorer (MS15-124)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Internet Explorer. These vulnerabilities could allow an attacker to execute code in the context of the browser if a user views a specially crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. 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.

THREAT INTELLIGENCE:
One memory corruption vulnerability (CVE-2015-6164) has been publicly disclosed.

SYSTEM AFFECTED:
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

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:
Microsoft Internet Explorer is prone to multiple vulnerabilities that could allow remote code execution. The vulnerabilities are as follows:
- 23 memory corruption vulnerabilities could allow for remote code execution.
- Two information disclosure vulnerabilities.
- One scripting engine memory corruption vulnerabilities that could allow for remote code execution.
- Three XSS filter bypass vulnerabilities that could lead to information disclosure
- One VBScript and Jscript ASLR Bypass vulnerability.

The most severe of these vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a specially crafted malicious website. When the website is visited, the attacker's script will run within the context of the affected browser or with the same permissions as the affected user account. 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.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:
Microsoft:
https://technet.microsoft.com/en-us/library/security/MS15-124

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6083
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6134
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6135
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6136
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6138
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6139
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6140
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6141
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6142
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6143
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6144
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6145
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6146
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6147
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6148
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6149
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6150
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6151
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6152
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6153
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6154
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6155
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6156
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6157
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6158
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6159
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6160
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6161
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6162
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6164

TLP: WHITE

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

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