

*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:

10/13/2015

10/30/2015 - Updated

SUBJECT:

Cumulative Security Update for Internet Explorer (MS15-106)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer. The most severe of 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.

October 30 – UPDATED OVERVIEW:

An additional vulnerability has been reported in Internet Explorer that could allow for remote code execution.

THREAT INTELLIGENCE:

One memory corruption vulnerability (CVE-2015-6056) has been publicly disclosed.

SYSTEMS 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 the most severe of which could allow remote code execution. The vulnerabilities are as follows:

- Four memory corruption vulnerabilities could allow for remote code execution.
- Three information disclosure vulnerabilities.
- Three scripting engine memory corruption vulnerabilities that could allow for remote code execution.
- Three elevation of privilege vulnerabilities.
- 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.

#### October 30 – UPDATED TECHNICAL SUMMARY:

Internet Explorer 11 is vulnerable to a memory corruption vulnerability that could allow for remote code execution. This vulnerability only affects Internet Explorer installations on Windows 10. (CVE-2015-6045)

#### RECOMMENDATIONS:

The following actions should be taken:

- Configure Internet Explorer to prompt before running Active Scripting or disable Active Scripting in the Internet and local intranet security zone until a patch is released.
- Apply updates as soon as possible 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/library/security/MS15-106>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2482>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6042>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6044>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6046>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6047>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6048>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6049>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6050>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6051>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6052>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6053>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6055>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6056>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6059>

October 30- UPDATED REFERENCES

Security Focus:

<http://www.securityfocus.com/bid/76985>

TLP: WHITE

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

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