

*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:**

06/14/2016

**SUBJECT:**

Cumulative Security Update for Internet Explorer (MS16-063)

**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. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then 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.

**SYSTEMS AFFECTED:**

- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Microsoft Internet Explorer is prone to multiple vulnerabilities that could allow remote code execution. The vulnerabilities are as follows:

- Five Scripting Engine Memory Corruption vulnerabilities exist in the way Jscript engines render when handling objects (CVE-2016-3202, CVE-2016-3205, CVE-3206, CVE-2016-3207, CVE-2016-3210)

- Three Microsoft Internet Explorer Memory Corruption vulnerabilities exist when Internet Explorer improperly access objects in memory (CVE-2016-0199, CVE-2016-0200, CVE-2016-3211)
- One Internet Explorer XSS Filter vulnerability exists when XSS Filter does not properly validate JavaScript (CVE-2016-3212)
- One WPAD Elevation of Privilege vulnerability (CVE-2016-3213)

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 patches provided by Microsoft 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 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:**

<http://technet.microsoft.com/en-us/library/security/mt720582.aspx>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0199>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0200>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3202>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3205>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3206>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3207>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3210>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3211>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3212>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3213>

#### **TLP: WHITE**

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

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