

*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:**

09/13/2016

**SUBJECT:**

Cumulative Security Update for Internet Explorer (MS16-104)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Internet Explorer the most severe of which could allow remote code execution if a user views a specially crafted web page. An attacker who successfully exploited these 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:

- Four memory corruption vulnerabilities exist when Internet Explorer improperly accesses objects in memory (CVE-2016-3247, CVE-2016-3295, CVE-2016-3297, CVE-2016-3324)
- Two information disclosure vulnerabilities exist when Internet Explorer improperly handles objects in memory (CVE-2016-3325, CVE-2016-3351)
- One remote code execution vulnerability exists in the way that the Microsoft OLE Automation mechanism and the VBScript Scripting Engine in Internet Explorer access objects in memory (CVE-2016-3375)
- One information disclosure vulnerability exists when Internet Explorer improperly handles cross-origin requests (CVE-2016-3291)
- One security feature bypass vulnerability exists when Internet Explorer handles files from the Internet zone (CVE-2016-3353)
- One privilege escalation vulnerability exists when Internet Explorer fails a check allowing a sandbox escape (CVE-2016-3292)

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. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. 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 by Microsoft 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.
- Apply the principle of Least Privilege to all systems and services.

#### **REFERENCES:**

##### **Microsoft:**

<https://technet.microsoft.com/library/security/MS16-104>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3247>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3291>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3292>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3295>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3297>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3324>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3325>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3351>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3353>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3375>

**TLP: WHITE**

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

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