

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:

02/09/2016

SUBJECT:

Cumulative Security Update for Internet Explorer (MS16-009)

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 this vulnerability could gain the same user rights as the current user. Depending on the privileges associated with the user, an attacker may install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are no reports of these vulnerabilities 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: **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 most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability 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. The vulnerabilities are as follows:

- One remote code execution vulnerability exists when Internet Explorer improperly validates input before loading dynamic link library (DLL) files. (CVE-2016-0041)
- One information disclosure vulnerability exists in Internet Explorer when Hyperlink Object Library improperly discloses the contents of its memory. (CVE-2016-0059)
- Eight remote code execution vulnerabilities exist when Internet Explorer improperly accesses objects in memory. (CVE-2016-0060, CVE-2016-0061, CVE-2016-0062, CVE-2016-0063, CVE-2016-0064, CVE-2016-0067, CVE-2016-0071, CVE-2016-0072)
- One spoofing vulnerability exists when a Microsoft browser does not properly parse HTTP responses. (CVE-2016-0077)
- Two elevation of privilege vulnerabilities exist when Internet Explorer does not properly enforce cross-domain policies. (CVE-2016-0068, CVE-2016-0069)

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 un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-009.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0041>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0059>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0060>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0061>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0062>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0063>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0064>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0067>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0068>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0069>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0070>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0071>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0072>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0077>

TLP: WHITE

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

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

