

*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:**

03/08/2016

**SUBJECT:**

Cumulative Security Update for Microsoft Edge (MS16-024)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Edge that could allow for remote code execution. Microsoft Edge replaced Internet Explorer as the default browser on Windows 10. 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:**

There are no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Microsoft Edge

**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:**

Multiple vulnerabilities have been discovered in Microsoft Edge that could allow for remote code execution.

- Ten remote code execution vulnerabilities exist when Microsoft Edge improperly accesses objects in memory. These vulnerabilities could allow an attacker to execute arbitrary code in the context of the user by luring a victim to view a webpage containing malicious code. (CVE-2016-0102, CVE-2016-0105, CVE-2016-0109, CVE-2016-0110, CVE-2016-0111, CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, CVE-2016-0129, CVE-2016-0130)
- An information disclosure vulnerability exists in Microsoft Edge when the referrer policy is improperly handled. An attacker who successfully exploited the vulnerability could gain information about the request context or browsing history of a user. To exploit the vulnerability,

an attacker must convince a victim who is accessing a secure website to click a link that takes the victim to a malicious website. (CVE-2016-0125)

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.

#### **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/ms16-024.aspx>

##### **CVE:**

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0102>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0105>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0109>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0110>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0111>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0116>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0123>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0124>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0125>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0129>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0130>

#### **TLP: WHITE**

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

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