

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 Microsoft Edge (MS16-011)

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:

- Windows 10

RISK:

Government: High

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

Businesses: High

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

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Microsoft Edge that could allow for remote code execution. Details of these vulnerabilities are as follows:

- A Microsoft browser spoofing vulnerability exists that could allow a browser to be redirected to a malicious website. (CVE-2016-007)
- A security feature bypass vulnerability exists that could be used in conjunction with another vulnerability to run arbitrary code (CVE-2016-0080)
- Multiple memory corruption vulnerabilities exist that could allow arbitrary code execution. (CVE-2016-0060, CVE-2016-0061, CVE-2016-0062, CVE-2016-0084)

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. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative 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/ms16-011.aspx>

CVE:

<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-2016-0077>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0080>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0084>

TLP: WHITE

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

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