

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:

08/11/2015

SUBJECT:

Cumulative Security Update for Microsoft Edge (MS15-091)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Edge, the most severe of which 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:

- 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:

Multiple vulnerabilities exist in Microsoft Edge due to the way objects in memory are improperly accessed. The vulnerabilities are as follows:

- Three Memory Corruption Vulnerabilities (CVE-2015-2441, CVE-2015-2442, CVE-2015-2446)
- One ASLR Bypass Vulnerability (CVE-2015-2449)

These vulnerabilities could allow an attacker to execute remote code by luring a victim to a malicious website. When the website is visited, the attacker's script will run with the same permissions as the affected user account. Successful exploitation of these vulnerabilities could result in an attacker gaining elevated privileges on the system. 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/library/security/MS15-091>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2441>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2442>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2446>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2449>

TLP: WHITE

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

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