

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

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

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

DATE(S) ISSUED:

11/08/2016

SUBJECT:

Cumulative Security Update for Microsoft Edge (MS16-129)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Edge, the most severe of which could allow remote code execution if a user views a specially crafted web page. 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:

An information disclosure (CVE-2016-7199) and a spoofing (CVE-2016-7204) vulnerability have been publicly disclosed. There are also reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Windows 10
- Windows 10 (Version 1511)
- Windows 10 (Version 1607)
- Windows Server 2016

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, the most severe of which could allow for remote code execution if a user views a specially crafted web page. Details of these vulnerabilities are as follows:

- Eight scripting engine memory corruption vulnerabilities exist in the way the scripting engine renders when handling objects in memory. (CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, CVE-2016-7243)
- Four memory corruption vulnerabilities exist when Microsoft Edge improperly handles objects in memory. (CVE-2016-7195, CVE-2016-7196, CVE-2016-7198, CVE-2016-7241)
- Three information disclosure vulnerabilities exist when Microsoft Edge improperly handles objects in memory. (CVE-2016-7199, CVE-2016-7204, CVE-2016-7227)
- One information disclosure vulnerability exists when the Microsoft Edge XSS filter is abused to leak sensitive page information. (CVE-2016-7239)
- One spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content. (CVE-2016-7209)

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.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-129.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7195>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7196>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7198>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7199>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7200>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7201>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7202>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7203>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7204>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7208>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7209>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7227>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7239>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7240>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7241>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7242>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7243>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

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