

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 ISSUED:

08/11/2015

SUBJECT:

Cumulative Security Update for Internet Explorer (MS15-079)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer. These vulnerabilities could allow an attacker to execute code in the context of the browser. 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. Failed attempts will result in denial of service conditions.

THREAT INTELLIGENCE:

The memory corruption vulnerabilities, which allow for remote code execution have not been publicly disclosed. The vulnerability related to the unsafe command line parameter passing has been publicly disclosed.

SYSTEM AFFECTED:

- Internet Explorer 7
- Internet Explorer 8
- 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 vulnerabilities are as follows:

- 10 memory corruption vulnerabilities could allow for remote code execution.
- Two ASLR bypass vulnerabilities could allow an attacker to more reliably run arbitrary code on the vulnerable system in the context of the affected user.
- One unsafe command line parameter passing vulnerability which could allow for disclosure of information.

These vulnerabilities could allow an attacker to execute remote code by luring a victim to visit a malicious website. When the website is visited, the attacker's script will run within the context of the affected browser or with the same permissions as the affected user account. 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. Failed attempts will result in denial of service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Configure Internet Explorer to prompt before running Active Scripting or disable Active Scripting in the Internet and Local intranet security zone until a patch is released.
- Apply updates as soon as possible after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS15-079>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2423>

<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-2015-2443>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2444>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2445>

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

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2447>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2448>

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

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2450>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2451>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2452>

TLP: WHITE

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

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