

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:

07/14/15

SUBJECT:

Cumulative Security Update for Internet Explorer (MS15-065)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. 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.

THREAT INTELLIGENCE:

There is no known proof-of-concept code available at this time. Updates are available.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

RISK:

Government:

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

Businesses:

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

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities were discovered in Internet Explorer due to the way objects in memory are improperly accessed. The vulnerabilities are as follows:

- 19 Memory Corruption Vulnerabilities (CVE-2015-1733, CVE-2015-1738, CVE-2015-1767, CVE-2015-2383, CVE-2015-2384, CVE-2015-2385, CVE-2015-2388, CVE-2015-2389, CVE-2015-2390, CVE-2015-2391, CVE-2015-2397, CVE-2015-2401, CVE-2015-2403, CVE-2015-2404, CVE-2015-2406, CVE-2015-2408, CVE-2015-2411, CVE-2015-2422, CVE-2015-2425)
- 5 Information Disclosure Vulnerabilities (CVE-2015-1729, CVE-2015-2410, CVE-2015-2412, CVE-2015-2413, CVE-2015-2414)
- One Elevation of Privilege Vulnerability (CVE-2015-2402)
- One ASLR Bypass Vulnerability (CVE-2015-2419)
- One Cross Site Scripting Filter Bypass Vulnerability (CVE-2015-2398)
- One Jscript9 Memory Corruption Vulnerability (CVE-2015-2419)
- One VBScript Memory Corruption Vulnerability (CVE-2015-2372)

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 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 click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS15-065>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1729>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1733>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1738>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1767>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2372>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2383>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2384>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2385>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2388>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2389>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2390>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2391>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2397>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2398>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2401>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2402>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2403>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2404>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2406>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2408>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2410>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2411>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2412>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2413>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2414>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2419>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2421>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2422>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2425>

TLP: WHITE

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

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