

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.

DATE(S) ISSUED:

07/08/2014

SUBJECT:

Cumulative Security Update for Internet Explorer (MS14-037)

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 This advisory covers one public and twenty-three privately disclosed vulnerabilities. There has not been any active exploitation or exploit code observed for any of these vulnerabilities at the time of their announcement.

SYSTEM AFFECTED:

- Internet Explorer 6
- 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:

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

- Twenty-three memory corruption vulnerabilities
- One Certificate Security Feature Bypass vulnerability

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://support.microsoft.com/kb/2975687>

<https://technet.microsoft.com/library/security/ms14-037>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1763>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1765>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2783>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2785>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2786>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2787>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2788>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2789>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2790>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2791>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2792>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2794>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2795>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2797>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2798>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2800>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2801>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2802>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2803>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2804>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2806>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2807>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2809>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2813>