

*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:**

07/09/2013

09/13/2013 - **Updated**

**SUBJECT:**

Cumulative Security Update for Internet Explorer (MS13-055)

**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 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.

**SYSTEMS AFFECTED:**

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 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**

**DESCRIPTION:**

Multiple vulnerabilities have been discovered in Internet Explorer. The details of these vulnerabilities are as follows:

Shift JIS Character Encoding Vulnerability: A cross-site-scripting (XSS) vulnerability exists in Internet Explorer that could allow information disclosure. An attacker could exploit the vulnerability by constructing a specially crafted webpage that could allow information disclosure if a user viewed the webpage. An attacker who successfully exploited this vulnerability could view content from another domain or Internet Explorer zone.

Multiple Memory Corruption Vulnerabilities: Multiple remote code execution vulnerabilities exist when Internet Explorer improperly accesses an object in memory. These vulnerabilities may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

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.

**September 13 – UPDATED DESCRIPTION:**

***Microsoft has updated security bulletin MS13-055 to include an additional vulnerability that was addressed by this update. The vulnerability addressed is CVE-2013-3846, a memory corruption vulnerability that could result in remote code execution.***

**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 from un-trusted sources.

**REFERENCES:**

**Microsoft:**

<http://support.microsoft.com/kb/2846071>

<http://technet.microsoft.com/en-us/security/bulletin/ms13-055>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3166>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3115>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3143>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3144>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3145>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3146>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3147>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3148>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3149>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3150>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3151>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3152>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3153>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3161>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3162>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3163>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3164>

**September 13 - UPDATE REFERENCES:**

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3846>