

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:

08/13/2013

SUBJECT:

Cumulative Security Update for Internet Explorer (MS13-059)

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:

Internet Explorer Process Integrity Level Assignment Vulnerability: An elevation of privilege vulnerability exists in Internet Explorer that could allow arbitrary code execution. This vulnerability could be used in conjunction with another vulnerability that allowed remote code execution. Utilizing the two vulnerabilities, an attacker could cause the arbitrary code to run at an elevated permission level. An attacker who successfully exploited this vulnerability could elevate the privileges of a process that is launched by Internet Explorer to run in the security context of the current user.

EUC-JP 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 perform cross-site scripting attacks, resulting in information disclosure when a user viewed a target website.

Multiple Memory Corruption Vulnerabilities: Multiple memory corruption vulnerabilities exist due to Internet Explorer improperly accessing objects 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.

REFERENCES:

Microsoft:

<https://support.microsoft.com/kb/2862772>

<http://technet.microsoft.com/en-us/security/bulletin/ms13-059>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3186>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3192>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3184>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3187>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3188>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3189>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3190>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3191>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3193>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3194>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3199>

Security Focus:

<http://www.securityfocus.com/bid/61679>

<http://www.securityfocus.com/bid/61680>

<http://www.securityfocus.com/bid/61677>

<http://www.securityfocus.com/bid/61675>

<http://www.securityfocus.com/bid/61669>

<http://www.securityfocus.com/bid/61663>

<http://www.securityfocus.com/bid/61670>

<http://www.securityfocus.com/bid/61664>

<http://www.securityfocus.com/bid/61668>

<http://www.securityfocus.com/bid/61671>

<http://www.securityfocus.com/bid/61678>