

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:

06/14/2011

SUBJECT:

Cumulative Security Update for Internet Explorer (MS11-050)

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. Several of the vulnerabilities can also lead to information disclosure if successfully exploited.

SYSTEMS AFFECTED:

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

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:

Eleven vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

Memory Corruption Vulnerabilities

Eight remote code execution vulnerabilities exist in the way Internet Explorer accesses objects in memory that have not been properly initialized or deleted. These vulnerabilities may be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerabilities. An alternative attack vector is possible if an attacker could embed an ActiveX control that is marked 'safe for initialization' in an application or Microsoft Office document that hosts the IE rendering engine. Successful exploitation of any 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.

Information Disclosure Vulnerabilities

Three information disclosure vulnerabilities have also been discovered in Internet Explorer. An attacker who successfully exploited any of these vulnerabilities, by convincing a user to visit a specially crafted website, could potentially access information in other domains or Internet Explorer Zones.

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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms11-050.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1246>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1250>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1251>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1252>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1254>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1255>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1256>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1258>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1260>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1261>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1262>

SecurityFocus:

<http://www.securityfocus.com/bid/48199>

<http://www.securityfocus.com/bid/48200>

<http://www.securityfocus.com/bid/48201>

<http://www.securityfocus.com/bid/48202>

<http://www.securityfocus.com/bid/48203>

<http://www.securityfocus.com/bid/48204>

<http://www.securityfocus.com/bid/48205>