

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:

10/11/2011

SUBJECT:

Cumulative Security Update for Internet Explorer (MS11-081) - RISK: HIGH

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

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:

Eight memory corruption vulnerabilities exist in Internet Explorer due to the way it accesses objects in memory that have not been properly initialized or deleted. Exploitation of any of these vulnerabilities may result in remote code execution. 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 also possible. 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 taking complete control of the system.

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 or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms11-081.msp>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1993>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1995>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1996>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1997>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1998>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1999>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2000>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2001>

SecurityFocus:

<http://www.securityfocus.com/bid/49947>

<http://www.securityfocus.com/bid/49960>

<http://www.securityfocus.com/bid/49961>

<http://www.securityfocus.com/bid/49962>

<http://www.securityfocus.com/bid/49963>

<http://www.securityfocus.com/bid/49965>

<http://www.securityfocus.com/bid/49966>

<http://www.securityfocus.com/bid/49967>