

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:

6/8/2010

SUBJECT:

Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS10-035)

OVERVIEW:

Six vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of these vulnerabilities. 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:

- Windows 2000
- Windows 2003
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2008
- Internet Explorer 5
- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

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:

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

Cross-Domain Information Disclosure Vulnerability

An information disclosure vulnerability exists in the way that Internet Explorer caches data and incorrectly allows the cached content to be called, potentially bypassing Internet Explorer domain restriction.

Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this

vulnerability. Successful exploitation of this vulnerability could result in an attacker viewing content from the local computer or another browser window in another domain or Internet Explorer zone.

toStaticHTML Information Disclosure Vulnerability

An information disclosure vulnerability exists in the way that Internet Explorer handles content using specific strings when sanitizing HTML. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in cross-site scripting allowing an attacker to execute script in the user's security context against a site that is using the toStaticHTML API.

Two Uninitialized Memory Corruption Vulnerabilities

Two remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. 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.

HTML Element Memory Corruption Vulnerability

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted in the IE8 Developer Toolbar. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. When a user views the web page, the vulnerability could allow remote code execution. Successful exploitation of this vulnerability 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.

Memory Corruption Vulnerability

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. When a user views the Web page, the vulnerability could allow remote code execution. Successful exploitation of this vulnerability 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.

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://www.microsoft.com/technet/security/bulletin/ms10-035.msp>

<http://blogs.technet.com/b/msrc/>

CVE: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0255>