

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:

12/8/2009

SUBJECT:

Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS09-072)

OVERVIEW:

Five 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 a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation 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:

- Microsoft Internet Explorer 5
- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7
- Microsoft 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:

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

ATL COM Initialization Vulnerability

A remote code execution vulnerability exists in an ActiveX control that is built with vulnerable Microsoft Active Template Library (ATL) headers. ATL allows a developer to create custom objects to quickly interface with Component Object Model (COM) features, such as ActiveX controls. Only components and controls that were built using Visual Studio ATL are

directly affected by this vulnerability. Such components and controls could allow the instantiation of arbitrary objects that could bypass related security policies. An attacker could exploit this vulnerability by constructing a specially crafted web page. When a user views the web page, the vulnerability could allow for remote code execution.

HTML Object Memory and Uninitialized Memory Corruption Vulnerabilities

Four remote code execution vulnerabilities exist in the way Internet Explorer accesses an object that has not been correctly initialized or deleted. An attacker could exploit these vulnerabilities by constructing a specially crafted web page. When a user views the web page, the vulnerability could allow for remote code execution.

Successful exploitation of any of these vulnerabilities could allow an attacker to execute arbitrary code on the affected system. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

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.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/ms09-072.mspx>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2493>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3671>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3672>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3673>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3674>

Security Focus:

<http://www.securityfocus.com/bid/35828>

<http://www.securityfocus.com/bid/37212>

<http://www.securityfocus.com/bid/37213>

<http://www.securityfocus.com/bid/37085>

<http://www.securityfocus.com/bid/37188>