

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:

04/09/2013

SUBJECT:

Vulnerability in MS Remote Desktop Client Could Allow Remote Code Execution (MS13-029)

ORIGINAL OVERVIEW:

A vulnerability has been discovered in Microsoft Remote Desktop Client that could allow for remote code execution. Remote desktop client is installed on Microsoft Windows operating systems by default, and is used to remotely log in to systems hosting the remote desktop service.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

AFFECTED SYSTEMS:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2

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:

A vulnerability has been discovered in Microsoft Remote Desktop Client that could allow for remote code execution. This vulnerability is caused when the Microsoft Remote Desktop ActiveX Control, mstscax.dll, attempts to access an object in memory that has been freed. This leads to the corruption of memory in such a way as to allow an attacker to execute arbitrary code in the context of the current user.

In order to exploit this vulnerability, an attacker could host a specially crafted website that is designed to exploit this vulnerability. The attacker would need to convince the victim to actively visit their website. When the user visits the malicious website, the attacker's code runs on the victim's system with the user's credentials.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could 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.

- If there is no business case, consider disabling or restricting access to the Microsoft Remote Desktop ActiveX Control (mstscax.dll).

- In Internet Explorer, consider setting the Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones

- 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:

<https://technet.microsoft.com/en-us/security/bulletin/ms13-029>

SecurityFocus:

<http://www.securityfocus.com/bid/58874>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1296>