

*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:**

11/05/2013

**12/10/2013 - UPDATE**

**SUBJECT:** Vulnerability in Microsoft Graphic Component could Allow Remote Code Execution

**OVERVIEW:**

A vulnerability has been found in the Microsoft Graphics component which could allow remote code execution in Microsoft Windows, Microsoft Office, and Microsoft Lync. Microsoft Windows is a popular operating system for both workstations and servers. Microsoft Office is an office suite of desktop applications. Microsoft Lync is a unified communications platform.

Successful exploitation of this vulnerability could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. 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.

~~**Please note that currently there are no security patches available to resolve this issue.**~~

Additionally, Microsoft is currently aware of targeted attacks that are trying to exploit this vulnerability.

**UPDATED OVERVIEW:**

***A patch has been released in Microsoft security bulletin MS13-096.***

**SYSTEMS AFFECTED:**

- . Windows Vista
- . Windows Server 2008
- . Windows Server Core 2008
- . Microsoft Office 2003
- . Microsoft Office 2007
- . Microsoft Office 2010
- . Microsoft Office Compatibility
- . Microsoft Lync 2010
- . Microsoft Lync 2013
- . Microsoft Lync Basic 2013

## **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 found in the Microsoft Graphics component which could allow remote code execution in Microsoft Windows, Microsoft Office, and Microsoft Lync. This vulnerability exists because of the way affected components handle specially crafted TIFF images. An attacker could exploit this vulnerability by convincing a user to preview or open a specially crafted email message, open a specially crafted file, or browse specially crafted web content.

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. 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.

~~**Please note that currently there are no security patches available to resolve this issue.**~~

Additionally, Microsoft is currently aware of targeted attacks that are trying to exploit this vulnerability.

### **UPDATED DESCRIPTION:**

***A patch has been released in Microsoft security bulletin MS13-096.***

## **RECOMMENDATIONS:**

The following actions should be taken:

- Microsoft recommends disabling the TIFF Codec as a workaround until a patch has been issued.
- Consider using the Microsoft Fix it solution: <https://support.microsoft.com/kb/2896666>
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

### **UPDATED RECOMMENDATIONS:**

**We recommend the following actions be taken:**

- **Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.**

**REFERENCES:**

**Microsoft:**

<http://technet.microsoft.com/en-us/security/advisory/2896666>

<https://support.microsoft.com/kb/2896666>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3906>

**SecurityFocus:**

<http://www.securityfocus.com/bid/63530>

**UPDATED REFERENCES:**

**Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/MS13-096>

<http://technet.microsoft.com/en-gb/security/advisory/2896666>