

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:

04/13/2011

SUBJECT:

Vulnerability in GDI+ Could Allow Remote Code Execution (MS11-029)

OVERVIEW:

A vulnerability has been discovered in the Microsoft Graphics Device Interface (GDI+). Microsoft Windows GDI+ enables various applications to display images. Microsoft GDI+ is installed by default on all Microsoft Windows operating systems. This vulnerability can be exploited if a user views a malicious web page, views or previews a malicious email message, or opens an email attachment containing a specially crafted image file designed to exploit the vulnerability.

Successful exploitation will result in an attacker gaining the same privileges as the logged on user. 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.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Microsoft Office XP

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:

Microsoft GDI+ is vulnerable to remote code execution because of the way it handles integer calculations. Specifically, this vulnerability involves how GDI+ processes enhanced meta file (.emf) images. The dynamic link library responsible for handling these GDI+ functions is "gdiplus.dll".

This vulnerability can be exploited if a user views a malicious web page, views or previews a document containing specially crafted image content, or opens an email attachment containing a specially crafted image file designed to exploit this vulnerability.

Successful exploitation will result in an attacker gaining the same privileges as the logged on user. 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.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS11-029.msp>

Security Focus:

<http://www.securityfocus.com/bid/47250>

Secunia:

<http://secunia.com/advisories/44155>

Vupen:

<http://www.vupen.com/english/advisories/2011/0946>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0041>