

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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

04/14/2015

SUBJECT:

Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (MS15-035)

OVERVIEW:

A vulnerability has been discovered in the way Microsoft Windows Graphics Component processes specially crafted Enhanced Metafile (EMF) image formats which could allow an attacker to take complete control of an affected system. EMF files provide a way to store pictures independent from the device on which they are displayed which guarantees the images will maintain their shape and proportion on any output device. 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.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2008 Core Installation

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

TECHNICAL SUMMARY:

A vulnerability has been privately reported in Microsoft Windows Graphics Component which could allow remote code execution if a user views a specially crafted Enhanced Metafile (EMF) image format file. This vulnerability can be exploited in a number of ways. An attacker could exploit this vulnerability through Internet Explorer by hosting websites or taking advantage of compromised websites and websites that accept or host user-provided content or advertisements to host a specially crafted EMF file. An attacker could exploit the vulnerability by sending Outlook users a specially crafted email or a specially crafted Office document as an attachment. An attacker could also exploit this vulnerability through Windows Explorer by hosting a malicious image file on a network share.

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.

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, follow links, or open attachments 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:

<https://technet.microsoft.com/en-us/security/bulletin/ms15-035>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1645>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp>