

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:

2/11/2014

SUBJECT:

Vulnerability in Direct2D Could Allow Remote Code Execution (MS14-007)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Microsoft's Direct2D, which could allow an attacker to take complete control of an affected system. Direct2D is a hardware-accelerated, immediate-mode 2-D graphics Application Programming Interface (API) that provides high performance and high-quality rendering for 2-D geometry, bitmaps, and text. Successful exploitation of this vulnerability 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:

At this time these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Windows 7
- Windows 8 and Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012 and Windows Server 2012 Rd
- Windows RT and Windows RT 8.1

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:

The vulnerability is caused when Direct2D fails to properly handle a specially crafted 2D geometric figure. An attacker could exploit this vulnerability by hosting a specially crafted website that is designed to invoke Direct2D through Internet Explorer.

An attacker who successfully exploited this vulnerability could cause arbitrary code to run with the privileges of the user who opens a specially crafted file or browses a website that contains specially crafted content. If the user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. 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 click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:**Microsoft:**

<https://technet.microsoft.com/en-us/security/bulletin/ms14-007>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0263>