



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 11, 2014

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2014-017

DATE(S) ISSUED:

03/11/2014

SUBJECT:

Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (MS14-013)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Microsoft DirectShow that could allow a remote attacker to take complete control of a vulnerable system. DirectShow is a component of Windows for streaming media and is used to perform various operations with media files on Microsoft Windows operating systems. This vulnerability can be exploited when a user opens a specially crafted JPEG image file. Successful exploitation could allow an attacker to gain 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, there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 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

TECHNICAL SUMMARY:

A vulnerability has been discovered in Microsoft DirectShow that could allow a remote attacker to take complete control of a vulnerable system. The vulnerability is caused by the DirectShow component improperly handling specially crafted Joint Photographic Experts Group (JPEG) image files. JPEG is one of the most common image file formats for image data. The specially crafted JPEG image file may be sent via email or hosted on a web site. This vulnerability can be leveraged with a web site that contains specially crafted content, or via an email containing an attachment of a specially crafted JPEG.

Successful exploitation could allow an attacker to gain 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:

We recommend the following actions 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 download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms14-013>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0301>