



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

August 14, 2012

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.

MS-ISAC ADVISORY NUMBER:

SA2012-049

DATE (S) ISSUED:

08/14/2012

SUBJECT:

Vulnerability in Microsoft Visio Could Allow Remote Code Execution (MS12-059)

OVERVIEW:

A vulnerability in Microsoft Visio has been identified that could allow for remote code execution. Microsoft Visio is a program commonly used to develop flowcharts, network diagrams and other visual media that can be used in Office-based products. 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.

SYSTEMS AFFECTED:

- Microsoft Visio Viewer 2010
- Microsoft Visio 2010

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: Medium

DESCRIPTION:

A vulnerability has been identified in Microsoft Visio that could result in remote code execution. This vulnerability exists due to the way Microsoft Visio parses specially crafted AutoCAD Interchange (.dxf) files. This particular vulnerability could allow for exploitation

through direct execution of the file or by visiting a website hosting a specially crafted DXF file.

In the email-based scenario, the user would have to open the specially crafted Visio file as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted Visio file that is hosted on the page.

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 visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

References:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms12-059>

SecurityFocus:

<http://www.securityfocus.com/bid/54934>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1888>