



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

April 13, 2011

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:
SA2011-026

DATE(S) ISSUED:
04/13/2011

SUBJECT:
Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (MS11-024)

OVERVIEW:
A vulnerability has been discovered in the Microsoft Windows Fax Cover Page Editor. Windows Fax Cover Page Editor enables users to create, modify, or view computer generated fax cover pages. Windows Fax Cover Page Editor is installed by default on Windows Vista Business Edition, Windows Vista Ultimate Edition, and in all supported editions of Windows 7. This vulnerability can be exploited if a user views a malicious web page, views a specially crafted Windows Fax Cover Page, or opens an email attachment containing a specially crafted image file designed to exploit the vulnerabilities.

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 7
- Windows Server 2003
- Windows Vista
- Windows Server 2008

RISK:
Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A memory corruption vulnerability has been discovered in the Windows Fax Cover Page Editor. This vulnerability exists due to Windows Fax Cover Page Editor improperly parsing fax cover pages (.cov) files. The vulnerability can be exploited if a user views a malicious web page, views a specially crafted Windows Fax Cover Page, or opens an email attachment containing a specially crafted 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.

It should be noted that in all supported editions of Windows XP, Vista Enterprise and Windows Server 2003, the Windows Fax Cover Page Editor is **not installed by default**. However, it is installed on Windows Vista Business and Windows Vista Ultimate Editions, and in all supported editions of Windows 7.

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.
- 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/MS11-024.mspx>

Security Focus:

<http://www.securityfocus.com/bid/45583>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3974>