

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

April 13, 2010

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:

SA2010-026

DATE(S) ISSUED:

4/13/2010

SUBJECT:

Vulnerabilities in Windows Could Allow Remote Code Execution (MS10-019)

OVERVIEW:

Two vulnerabilities have been discovered in the Microsoft Windows Authenticode Signature Verification function which could allow for remote code execution. Authenticode is a digital signature format that is used to determine the origin and integrity of software files. These vulnerabilities can be exploited when a user opens a specially crafted signed portable executable (PE) or cabinet file (CAB) which is a file that has been compressed, or reduced in size, to save storage space and allow faster transferring across a network. Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user, an attacker could then install programs; view, change, or delete data; or create new accounts.

SYSTEMS AFFECTED:

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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**DESCRIPTION:**

Two vulnerabilities have been discovered in the Microsoft Windows Authenticode Signature Verification function which could allow for remote code execution.

WinVerifyTrust Signature Validation Vulnerability

A remote code execution vulnerability exists in the Windows Authenticode Signature Verification function used for portable executable (PE) and cabinet file formats. An anonymous attacker could exploit the vulnerability by modifying an existing signed executable file to manipulate unverified portions of the file in such a way as to add malicious code to the file without invalidating the signature.

Cabview Corruption Validation Vulnerability

A remote code execution vulnerability exists in the Windows Authenticode Signature verification for cabinet (CAB) file formats. An attacker could exploit the vulnerability by modifying an existing signed cabinet file to point the unverified portions of the signature to malicious code, and then convince a user to open or view the specially crafted cabinet file.

Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user, an attacker could then install programs; view, change, or delete data; or create new accounts.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/ms10-019.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0486>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0487>