



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

February 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.

ADVISORY NUMBER:

SA2012-009

DATE(S) ISSUED:

02/14/2012

SUBJECT:

Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS12-008)

OVERVIEW:

Two vulnerabilities have been discovered in Microsoft Windows that could allow for remote code execution due to improper validation of input by a Windows kernel-mode driver. The vulnerable driver controls window displays, screen output, and input from devices which it passes to applications. Exploitation of these vulnerabilities could result in the execution of arbitrary code with full administrative privileges resulting in full control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

SYSTEMS AFFECTED:

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

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 identified in Microsoft Windows Kernel-Mode driver (win32.sys) that could allow for code execution. The first issue is a remote code execution vulnerability that is caused due to the way the Windows kernel mode driver handles input validation through the Graphical Device Interface (GDI). An attacker could leverage this vulnerability remotely by convincing a user to view a specially crafted website or email. The vulnerability could also be exploited locally by running a specially crafted application.

The second vulnerability requires authentication and can only be exploited locally via a specially crafted application. The vulnerability is triggered when the Windows kernel-mode driver improperly handles keyboard layout errors.

Successful exploitation of any of these vulnerabilities will result in an attacker gaining the ability to install programs; view, change, or delete data; or create new accounts with full administrative rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:**Microsoft:**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-008>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5046>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0154>

Security Focus:

<http://www.securityfocus.com/bid/51122>