



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

November 13, 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:

SA2012-071

DATE(S) ISSUED:

11/13/2012

SUBJECT:

Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS12-075)

OVERVIEW:

Three vulnerabilities have been discovered in Microsoft Windows Kernel-Mode drivers that could allow for remote code execution. The kernel mode drivers controls window displays, screen output, and input from devices that the kernel passes to applications. Exploitation of these vulnerabilities could result in the execution of arbitrary code with full system 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 Server 2008
- Windows 7
- Windows 8
- Windows Server 2012
- Windows RT

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:

Three vulnerabilities have been identified in Microsoft Windows Kernel-Mode driver (win32.sys) that could allow for code execution. The details of the vulnerabilities are as follows:

Win32k Use After Free Vulnerability (CVE-2012-2530, CVE-2012-2553):

Two of the vulnerabilities are elevation of privilege vulnerabilities that are due to the way the Windows kernel mode driver handles objects in memory. In order for successful exploitation to occur, an attacker must have valid logon credentials and be able to logon locally. Then, an attacker could run a specially crafted application and take complete control over the affected system.

TrueType Font Parsing Vulnerability (CVE-2012-2897)

The third vulnerability is caused when Windows font parsing improperly handles objects in memory. This vulnerability can be exploited by visiting a specially crafted webpage or opening a specially crafted file, such as an email attachment. In an email scenario the attacker would need the user to open an attachment or click a link to a specially crafted webpage.

Successful exploitation of any of these vulnerabilities could 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.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to download or open files from un-trusted websites.
- 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/ms12-075>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2530>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2553>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2897>

SecurityFocus:

<http://www.securityfocus.com/bid/56457>

<http://www.securityfocus.com/bid/56448>

<http://www.securityfocus.com/bid/56447>