



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

October 14, 2014

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:

SA2014-064

DATE(S) ISSUED:

10/14/2014

SUBJECT:

Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (MS14-058)

EXECUTIVE SUMMARY:

Two vulnerabilities have been identified in the Microsoft Windows kernel-mode driver that could allow for privilege escalation or remote code execution. The kernel-mode driver controls window displays, screen output, and input from devices that the kernel passes to applications. Successful exploitation of these vulnerabilities could result in the execution of arbitrary code with elevated privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

THREAT INTELLIGENCE

There are limited reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8 & Windows 8.1
- Windows Server 2012 & Windows Server 2012 R2
- Windows RT & Windows RT 8.1

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

TECHNICAL SUMMARY:

Two privately reported vulnerabilities have been identified in the Microsoft Windows Kernel-Mode driver that could allow for remote code execution. These vulnerabilities are as follows:

- **Win32k.sys Elevation of Privilege Vulnerability (CVE-2014-4113)** An elevation of privilege vulnerability exists when the Windows kernel-mode driver improperly handles objects in memory.
- **TrueType Font Parsing Remote Code Execution Vulnerability (CVE-2014-4148)** A remote code execution vulnerability exists when the Windows kernel-mode driver improperly handles TrueType fonts

Successful exploitation of these vulnerabilities could result in the execution of arbitrary code with elevated privileges. An attacker could then 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.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Adobe:

<https://technet.microsoft.com/en-us/library/security/ms14-058.aspx>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4113>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4148>