



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

September 8, 2015

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:
SA2015-112**

**DATE(S) ISSUED:
09/08/2015**

**SUBJECT:
Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution
(MS15-097)**

OVERVIEW:
Multiple vulnerabilities have been discovered in the Microsoft graphics component that could allow for remote code execution. Successful exploitation of these vulnerabilities could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE
Microsoft reports that one elevation of privilege vulnerability (CVE-2015-2546) has been publicly disclosed.

SYSTEMS AFFECTED:

- Windows Vista
- Windows 7
- Windows 8 and 8.1
- Windows Server 2008 including R2 (Server Core Installations are affected)
- Windows Server 2012 including R2 (Server Core Installations are affected)
- Windows RT 8 and RT 8.1
- Windows 10
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Lync 2010
- Microsoft Lync 2010 Attendee
- Microsoft Lync 2013
- Microsoft Lync Basic 2013

- **Microsoft Live Meeting 2007 Console**

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:

A graphic component buffer overflow vulnerability (CVE-2015-2510) has been discovered in Microsoft Windows, Office, and Microsoft Lync that could allow for remote code execution when handling specially crafted OpenType fonts.

Successful exploitation of this vulnerability could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker may exploit these vulnerabilities by redirecting users to a specially crafted webpage or by users opening a specially crafted document.

The Microsoft bulletin also patches the following unrelated vulnerabilities:

- **One OpenType Font Parsing (CVE-2015-2506).**
- **Multiple Font Driver Elevation of Privilege (CVE-2015-2507, CVE-2015-2508, CVE-2015-2512).**
- **Multiple Win32k Memory Corruption Elevation of Privileges (CVE-2015-2511, CVE-2015-2517, CVE-2015-2518, CVE-2015-2546).**

RECOMMENDATIONS:

We recommend the following actions be taken:

- **Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.**
- **If patching is not possible for CVE-2015-2510, workarounds are listed in the Microsoft reference below.**
- **Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.**
- **Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.**
- **Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.**
- **Workaround options are also available via the Microsoft link listed in the reference section**

REFERENCES:

Microsoft:

<https://technet.microsoft.com/library/security/MS15-097>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2506>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2507>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2508>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2510>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2511>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2512>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2517>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2518>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2527>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2529>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2546>