



# State of Alaska State Security Office

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

July 9, 2013

*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:**  
SA2013-058

**DATE(S) ISSUED:**  
07/09/2013

**SUBJECT:**

Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (MS13-057)

**OVERVIEW:**

A remote code execution vulnerability exists in Windows Media Format Runtime. Windows Media Format Runtime is a multimedia framework for media creation and distribution for Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted media file. An attacker who successfully exploits this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user 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:**

A remote code execution vulnerability exists in the way Windows Media Format Runtime handles certain media files. This occurs when Windows Media Player fails to properly parse specially crafted media files. This vulnerability could allow an attacker to execute arbitrary code if the attacker convinces a user to open a specially crafted media file. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Unless there is a business need to do otherwise, consider disabling Windows Media Player.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open email attachments from unknown or un-trusted sources.

**REFERENCES:**

**Microsoft:**

<http://support.microsoft.com/kb/2847883>

<https://technet.microsoft.com/en-us/security/bulletin/ms13-057>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3127>