

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

10/13/2015

SUBJECT:

Multiple Vulnerabilities in Windows Shell Could Allow Remote Code Execution (MS15-109)

OVERVIEW:

Multiple vulnerabilities have been discovered in Windows Shell which could allow an attacker to take complete control of an affected system. The Windows Shell is used to run applications and manage the Windows operating system. Exploitation occurs when a user opens a specially crafted file designed to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8 and Windows 8.1
- Microsoft Windows 10
- Microsoft Windows RT and RT 8.1
- Microsoft Windows Server 2008 and Server 2008 R2 (including Server Core installations)
- Microsoft Windows Server 2012 and Server 2012 R2 (including Server Core installations)

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 use after free remote code execution vulnerabilities exist when Windows Shell fails to properly handle objects in memory. An attacker could exploit this vulnerability by constructing a specially crafted file and attempting to convince a user to open it from an email message or access it from a webpage. When the user opens the malicious file, Windows Shell fails to properly handle the objects in memory, allowing the attacker to execute arbitrary shell commands without the knowledge of the logged on user. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Deny access to the "TipBand.dll" as a workaround (CVE-2015-2548).
- 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.
- 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 from un-trusted sources.

REFERENCES:**Microsoft:**

<https://technet.microsoft.com/library/security/MS15-109>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-2515>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE2015-2548>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>