

*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:**

09/08/2015

**SUBJECT:**

Multiple Vulnerabilities in Microsoft Windows Journal Could Allow Remote Code Execution (MS15-098)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft Windows Journal that could allow remote code execution. These vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Journal (.jnl) file. Successful exploitation of these vulnerabilities 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 no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Windows Vista
- Windows 7
- Windows 8 and Windows 8.1
- Windows RT and Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows 10

**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:**

Multiple vulnerabilities have been discovered in Microsoft Windows Journal which could allow for remote code execution when handling specially crafted Journal files. This update addresses four remote code execution vulnerabilities listed below:

- Windows Journal Remote Code Execution Vulnerability (CVE-2015-2513)
- Windows Journal Remote Code Execution Vulnerability (CVE-2015-2514)
- Windows Journal Integer Overflow Remote Code Execution Vulnerability (CVE-2015-2519)
- Windows Journal Remote Code Execution Vulnerability (CVE-2015-2530)

Additionally a Windows Journal Denial of Service Vulnerability (CVE-2015-2516) is addressed in this update.

Successful exploitation of these vulnerabilities could result in the attacker gaining the same rights 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. 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.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- If patching is not possible immediately multiple 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 from un-trusted sources.

#### **REFERENCES:**

##### **Microsoft:**

<https://technet.microsoft.com/library/security/ms15-098>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2513>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2514>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2519>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2530>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2516>

#### **TLP: WHITE**

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

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