

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:

11/10/2015

SUBJECT:

Vulnerability in Microsoft Windows Journal Could Allow Remote Code Execution (MS15-114)

OVERVIEW:

A heap overflow vulnerability has been discovered in Microsoft Windows Journal that could allow remote code execution. This vulnerability is triggered if a user opens a specially crafted Microsoft Journal (.jnt) file. 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 no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Windows Vista
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

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 heap overflow vulnerability has been discovered in Microsoft Windows Journal, which could allow for remote code execution when handling specially crafted Journal (.jnt) files. In an email attack scenario, an attacker could exploit this vulnerability by sending an email enticing a user to open an attached specially crafted Journal file. Successful exploitation of this vulnerability 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. (CVE-2015-6097)

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/en-us/library/security/ms15-114.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6097>

TLP: WHITE

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

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