

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:

02/09/2016

SUBJECT:

Vulnerabilities in Microsoft Windows PDF Library Could Allow for Remote Code Execution (MS16-012)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Windows PDF Library that could allow for remote code execution. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker may install applications, 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.

SYSTEMS AFFECTED:

- Windows 8.1, 10
- Windows Server 2012, 2012 R2 and 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 vulnerabilities have been reported in Microsoft Windows PDF Library. These vulnerabilities could allow for remote code execution. Details of these vulnerabilities are as follows:

- A remote code execution vulnerability exists in Microsoft Windows when a specially crafted file is opened in Windows Reader. (CVE-2016-0046)
- A buffer overflow vulnerability exists in Microsoft Windows PDF Library when it improperly handles application programming interface (API) calls. (CVE-2016-0058)

Successful exploitation could allow an attacker to gain 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:

- 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.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-012.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0046>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0058>

TLP: WHITE

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

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