

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:

08/09/2016

SUBJECT:

Vulnerability in Microsoft Windows PDF Library Could Allow for Remote Code Execution (MS16-102)

OVERVIEW:

A vulnerability has been discovered in Microsoft Windows PDF Library, which could allow for remote code execution. Windows PDF Library is a library used for natively reading PDF files, and is included in various Windows operating system installations. These vulnerabilities are triggered if a user opens a specially crafted PDF 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 currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Windows 8.1
- Windows RT 8.1
- Windows Server 2012, 2012 R2, and R2 Server Core installations
- Windows 10

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A remote code execution vulnerability exists when Microsoft Windows PDF Library improperly handles objects in memory. The vulnerability could corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. This vulnerability is triggered if a user opens a specially crafted PDF file. In an email attack scenario, an attacker could exploit this vulnerability by sending an email and enticing a user to open a specially crafted PDF file that is attached. (CVE-2016-3319)

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. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those 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.
- 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 those from un-trusted sources.
- Apply the principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-102.aspx>

CVE:

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3319>

TLP: WHITE

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

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