

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:

03/08/2016

SUBJECT:

Multiple Vulnerabilities in Microsoft Graphic Fonts Could Allow for Remote Code Execution (MS16-026)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Windows, the most severe of which could allow for remote code execution. These vulnerabilities can be exploited by either convincing a user to open a specially crafted document, or by convincing a user to visit a webpage that contains specially crafted embedded OpenType fonts. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user or result in a denial of service. 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.

SYSTEMS AFFECTED:

- Windows Vista
- Windows Server 2008, 2008 R2 & All Server Core installations
- Windows 7
- Windows 8.1, RT 8.1
- Windows Server 2012, 2012 R2 & All 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:

Multiple vulnerabilities exist in Microsoft Windows, the most severe of which could allow remote code execution. The vulnerabilities are as follows:

- A denial of service vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could cause a denial of service condition. For systems running Windows 10, an attacker who successfully exploited the vulnerability could potentially cause the application to stop responding instead of the system. (CVE-2016-0120)
- A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted fonts. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. 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. (CVE-2016-0121)

In order to exploit these vulnerabilities an attacker would have to convince a user to open a specially crafted document, or visit a webpage that contains specially crafted embedded OpenType fonts.

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 from untrusted sources.

REFERENCES:

Microsoft:

<https://technet.microsoft.com/en-us/library/security/ms16-026.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0120>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0121>

TLP: WHITE

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

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