

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**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

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

**DATE(S) ISSUED:**

05/14/2019

05/16/2019 – *UPDATED*

06/06/2019 - *UPDATED*

**SUBJECT:**

Critical Patches Issued for Microsoft Products, May 14, 2019

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for code execution. Successful exploitation of the most severe 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

***May 16 – UPDATED OVERVIEW:***

***Microsoft has released an additional bulletin highlighting a Critical level vulnerability affecting Windows 7 systems and below (CVE-2019-0708).***

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

***June 6 – UPDATED THREAT INTELLIGENCE:***

***Metasploit module exploiting CVE-2019-0708 to achieve remote code execution is currently available.***

**SYSTEMS AFFECTED:**

- Adobe Flash Player
- Microsoft Windows
- Internet Explorer
- Microsoft Edge
- Microsoft Office and Microsoft Office Services and Web Apps
- Team Foundation Server
- Visual Studio
- Azure DevOps Server
- SQL Server
- .NET Framework
- .NET Core

- ASP.NET Core
- ChakraCore
- Online Services
- Azure
- NuGet
- Skype for Android

**May 16 – UPDATED SYSTEMS AFFECTED**

- **Windows 7**
- **Windows Server 2008, 2008 R2**
- **Windows 2003**
- **Windows XP**

**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 have been discovered in Microsoft products, the most severe of which could allow for code execution.

A full list of all vulnerabilities can be found at the link below:

<https://portal.msrc.microsoft.com/en-us/security-guidance>

Successful exploitation of the most severe 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

**May 16 – UPDATED TECHNICAL SUMMARY:**

**Microsoft has released an additional bulletin highlighting a Critical level vulnerability affecting Windows 7 systems and below (CVE-2019-0708). This vulnerability exploits the Remote Desktop Protocol and allows for an unauthenticated attacker to connect to a system by sending specially crafted requests. Successful exploitation of this vulnerability could allow for remote code execution. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.**

**NOTE: This vulnerability was fixed in the May 14<sup>th</sup> patches released by Microsoft.**

**For more information on this vulnerability please reference the Microsoft Advisory below:**

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

## **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources
- Apply the Principle of Least Privilege to all systems and services.

## **REFERENCES:**

### **Microsoft:**

<https://portal.msrc.microsoft.com/en-us/security-guidance>

<https://portal.msrc.microsoft.com/en-us/security-guidance/summary>

<https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/e5989c8b-7046-e911-a98e-000d3a33a34d>

### **May 16 – UPDATED REFERENCES:**

#### **Microsoft:**

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

<https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708>

#### **KerbsonSecurity:**

<https://krebsonsecurity.com/2019/05/microsoft-patches-wormable-flaw-in-windows-xp-7-and-windows-2003/>

#### **BleepingComputers:**

<https://www.bleepingcomputer.com/news/security/microsoft-fixes-critical-remote-desktop-flaw-blocks-worm-malware/>

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

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

**Greg Nohra**

Enterprise Security Architect

MS Department of Information Technology Services

601-432-8009 | [www.its.ms.gov](http://www.its.ms.gov)



DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited