

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:

07/09/2019

SUBJECT:

Critical Patches Issued for Microsoft Products, July 09, 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.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- ASP.NET Core 2.1, 2.2
- Azure Automation
- Azure DevOps Server 2019.0.1
- ChakraCore
- Edge
- Internet Explorer 9, 10, 11
- Mail and Calendar
- .NET Framework 2.0, 3.0, 3.5, 4.5, 4.6, 4.8
- Team Foundation Server 2010, 2012, 2013, 2014, 2015, 2017, 2018
- Visual Studio 2010, 2012, 2013, 2015, 2017, 2019
- Windows 7, 10, 8.1, RT 8.1
- Windows RT 8.1
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019
- Windows Server 2012, 2012 R2, 2016, 2019 (Server Core installation)
- Windows Server, version 1803 (Server Core Installation)
- Windows Server, version 1903 (Server Core Installation)
- Azure IoT Edge
- Azure Kubernetes
- Excel 2010, 2013, 2013 RT, 2016
- Exchange Server 2010, 2013, 2016, 2019
- .IdentityModel 7.0.0

- Lync 2013
- Office 2010, 2013, 2013 RT, 2016, 2016 for Mac, 2019, 2019 for Mac
- Office 365 ProPlus
- Outlook 2010, 2013, 2016, Android, iOS
- SharePoint Enterprise Server 2013, 2016
- SharePoint Foundation 2010, 2013
- SharePoint Server 2019
- Skype Business 2016
- SQL Server 2014, 2016, 2017

RISK:

Government:

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

Businesses:

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

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/48293f19-d662-e911-a98e-000d3a33c573>

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/>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts

Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | 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