TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2019-092

DATE(S) ISSUED: 09/10/2019

SUBJECT: Critical Patches Issued for Microsoft Products, September 10, 2019

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote 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:
- Access 2010,2013,2016
- ASP.NET Core 2.1,2.2,3.0
- ChakraCore
- Edge
- Excel 2010, 2013, 2013 RT, 2016
- Exchange Server 2016, 2019
- Internet Explorer 10, 11, 9
- Lync Server 2013
- .NET Core 2.1, 2.2
- .NET Framework 3.5,3.5 AND 4.7.2,3.5 AND 4.8,4.5.2,4.6.2,4.6.2/4.7/4.7.1/4.7.2,4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2,4.7.1/4.7.2,4.7.2,4.7/4.7.1/4.7.2,4.8
- Office 2010,2013,2013 RT,2016,2019
- Office 2016 for Mac
- Office 2019 for Mac
- Office 365 ProPlus
- Project 2010, 2013, 2016
- Rome SDK 1.4.1
- SharePoint Enterprise Server 2013, 2016
- SharePoint Foundation 2010, 2013
- SharePoint Server 2019
- Visual Studio 2015 Update 3, 2017, 2017 version 15.9, 2019 version 16.0, 2019 version 16.2
- Windows 10, 10 version 1709, 7, 8.1, RT 8.1
- Windows Server (Core Installation) 2012 R2, 2012, 2016, 2019
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019
- Windows Server, version 1803 (Server Core Installation)
- Windows Server, version 1903 (Server Core Installation)
- Yammer Android

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.

RECOMMENDATIONS:

We recommend the following actions 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/24f46f0a-489c-e911-a994-000d3a33c573

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722