**TLP: WHITE**
**MS-ISAC CYBERSECURITY ADVISORY**

**MS-ISAC ADVISORY NUMBER:** 2018-126

**DATE(S) ISSUED:** 11/13/2018

**SUBJECT:** Critical Patches Issued for Microsoft Products, November 13, 2018

**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:**
- Azure App Service for Azure Stack
- ChakraCore
- Dynamics 365 (on-premises) version 8
- Edge
- Excel 2010, 2013, 2013 RT, 2016
- Excel Viewer 2007
- Internet Explorer 10, 11, 9
- Lync 2013
- Lync Basic 2013
- .NET Core 2.1
- Office 2010, 2013, 2013 RT, 2016, 2019
- Office for Mac 2016, 2019
- Office 365 ProPlus
- Office Compatibility Pack
- Office Web Apps 2010, 2013
- Office Web Apps Server 2013
- Outlook 2010, 2013, 2013 RT, 2016
- PowerShell Core 6.0, 6.1
- Project 2010, 2016
- Project Server 2013
- SharePoint Enterprise Server 2013, 2016
- SharePoint Foundation 2013
- SharePoint Server 2010,2019
- Skype Business 2016,2016 Basic
- Team Foundation Server 2017 Update 3.1, 2018 Update 1.1, 2018 Update 3, 2018 Update 3.1
- Windows 7, 8.1, RT 8.1, 10
- Windows RT 8.1
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019
- Windows Server (Core Installation) 2012 R2, 2012, 2016, 2019
- Word 2010, 2013, 2013 RT, 2016

**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/summary

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/summary
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/ff746aa5-06a0-e811-a978-000d3a33c573

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