MS-ISAC ADVISORY NUMBER:
2019-070

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
- Windows 7, 10, 8.1, RT 8.1
- Windows RT 8.1
- 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
- IdentityModel 7.0.0
- Lync 2013
- 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:

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:

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

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/