MS-ISAC ADVISORY NUMBER:
2019-106

DATE(S) ISSUED:
10/09/2019

SUBJECT:
Critical Patches Issued for Microsoft Products, October 08, 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:
- Azure App Service on Azure Stack
- ChakraCore
- Excel Services
- Internet Explorer 10, 11, 9
- Microsoft Dynamics 365
- Microsoft Edge (EdgeHTML-based)
- Microsoft Office 2010, 2013, 2016, 2019
- Microsoft SharePoint Enterprise Server 2013, 2016
- Microsoft SharePoint Foundation 2010, 2013
- Microsoft SharePoint Server 2019
- Office 365
- Office Online Server
- Open Enclave SDK
- SQL Server Management Studio 18.3, 18.3.1
- Windows 10, 7, 8.1
- Windows RT 8.1
- Windows Server, version 1803, 1903
- Windows Update Assistant

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:

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/releasenotedetail/28ef0a64-489c-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

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/