Date(S) Issued: 01/14/2020

Subject: Critical Patches Issued for Microsoft Products, January 14, 2020

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:
Critical vulnerability CVE-2020-0601 included in this roll up addresses a certificate validation vulnerability in the cryptographic library crypt32.dll that could allow for remote code execution.

Systems Affected:
- .NET Core 3.0, 3.1
- ASP.NET Core 2.1, 3.0, 3.1
- Dynamics 365 Field Service
- Internet Explorer 10, 11, 9
- Microsoft .NET Framework 3.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8
- Microsoft Office 2010, 2013, 2016, 2019
- Office 365
- Office Online Server
- One Drive for Android
- Windows 10, 7, 8.1
- Windows RT 8.1
- Windows Server, version 1803, 1903, 1909

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 remote 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:

NSA:
https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF

CVES:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601

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/

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.