TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2018-040 **– UPDATED**

DATE(S) ISSUED:
04/10/2018
04/26/2018 - UPDATED

SUBJECT:
Critical Patches Issued for Microsoft Products, April 10, 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.

April 26 - UPDATED THREAT INTELLIGENCE:
Proof-of-concept source code is now available for CVE-2018-1038, which has now been nicknamed "Total Meltdown" as it exploits the Microsoft patch for the Meltdown vulnerability. The April Microsoft Patch remediates both the "Total Meltdown" vulnerability and the proof-of-concept code.

SYSTEM AFFECTED:
- Microsoft Internet Explorer 9, 10, 11
- Microsoft Edge
- Microsoft Windows: 7 SP1, 8.1, RT 8.1, 10
- Microsoft Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Windows Server Core Installations: version 1709, 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Office 2010 SP2, 2013 RT SP1, 2013 SP1, 2016, 2016 C2R
- Microsoft Office Compatibility Pack SP3
- Microsoft Office Web Apps 2010 SP2
- Microsoft Office Web Apps Server 2013 SP1
- Microsoft Word 2007 SP3, 2010 SP2, 2013 RT SP1, 2013 SP1, 2016
- Microsoft Excel Viewer 2007 SP3
- Excel Services
- Microsoft Excel 2007 SP3, 2010 SP2, 2013 RT SP1, 2016
- Microsoft Outlook 2007, 2010 SP2, 2013 RT SP1, 2013 SP1, 2016
- Microsoft SharePoint Server 2010 SP2, 2013 SP1
- Microsoft SharePoint Enterprise Server 2013 SP1, 2016
- Microsoft Wireless Keyboard 850
- Word Automation Services
- ChakraCore

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/abf77563-8612-e811-a966-000d3a33a34d

April 26 - UPDATED REFERENCES:
ZD Net:
https://www.zdnet.com/article/it-must-patch-against-total-meltdown-now-the-source-code-is-on-github

GitHub
https://gist.github.com/xpn/bdb99cee8895bab4b1a0671696570d94

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