

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

**MS-ISAC ADVISORY NUMBER:**  
2018-001 - **UPDATED**

**DATE(S) ISSUED:**  
01/03/2018  
01/9/2018 – *UPDATED*  
**01/29/2018 - UPDATED**

**SUBJECT:**  
Critical Patches Issued for Microsoft Products, January 03, 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.

**January 9<sup>th</sup> – UPDATED OVERVIEW:**  
The January 9<sup>th</sup> release incorporates patches for additional vulnerabilities and is applicable to additional systems.

**THREAT INTELLIGENCE:**  
This out-of-band Microsoft update partially patches the Spectre and Meltdown vulnerabilities but firmware updates are also required. There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- Microsoft Internet Explorer 11
- Microsoft Edge
- Microsoft Windows: 7, 8.1, 10
- Microsoft Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft SQL Server: 2016, 2016 GDR, 2017, 2017 GDR

**January 9<sup>th</sup> – UPDATED SYSTEMS AFFECTED:**

- Microsoft Office: 2007, 2010, 2013, 2016
- SharePoint Server: 2010, 2013, 2016
- SharePoint Foundation: 2010, 2013
- .NET Framework: 2, 3, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1
- .NET Core
- ChakraCore
- ASP.NET Core

**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.

#### **January 29 – UPDATED TECHNICAL SUMMARY**

*Microsoft has released an out of band patch (KB4078130), which disables mitigations for CVE-2017-5715. This is in response to reports that the update mitigating CVE-2017-5715 resulted in unexpected reboots and other unexpected behavior that may lead to data loss or corruption. This patch only affects the mitigation against CVE-2017-5715, which was found to be the root cause of the unexpected behavior. Installation of this patch will remove the protections against CVE-2017-5715 on affected machines.*

*For those experiencing this behavior and who would like to apply this patch, Microsoft has made the patch available at the link below:*

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4078130>

#### 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> <https://portal.msrc.microsoft.com/en-us/security-guidance/summary>

#### **January 29 – UPDATED REFERENCES**

Microsoft:

<https://support.microsoft.com/en-us/help/4078130/update-to-disable-mitigation-against-spectre-variant-2>

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4078130>

24x7 Security Operations Center Multi-State Information Sharing and Analysis Center (MS-ISAC) 31  
Tech Valley Drive East Greenbush, NY 12061 [SOC@cisecurity.org](mailto: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/>