TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2017-083

DATE ISSUED:
09/12/2017

SUBJECT:
Critical Patches Issued for Microsoft Products, September 12, 2017

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:
CVE-2017-8759 is being actively used in the wild.

SYSTEMS AFFECTED:
- Internet Explorer 9, 10, 11
- Microsoft Lync 2010, Basic 2013
- Microsoft Edge
- Microsoft .NET Framework
- Microsoft Windows 7, 8.1, RT 8.1, 10
- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Office Web Apps 2010, 2013
- Microsoft Office 2007, 2010, 2011, 2013, 2013 RT, 2016
- Microsoft SharePoint Server 2007, 2010, 2013
- Microsoft Exchange Server 2013
- Microsoft Compatibility Pack
- Microsoft Word Viewer, Excel Viewer
- Microsoft Live Meeting 2007
- Skype for Business 2016

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:
https://portal.msrc.microsoft.com/en-us/security-guidance

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
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/5984735e-f651-e711-80dd-000d3a32fc99

FireEye:
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html

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