TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2017-055 ***- UPDATED***

DATE ISSUED:
06/13/2017
06/14/2017 - UPDATED

SUBJECT:
Critical Patches Issued for Microsoft Products, June 13, 2017

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.

June 14 - UPDATED THREAT INTELLIGENCE:
There have been reports of vulnerabilities related to The Shadow Brokers exploit releases being actively exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 9, 10, 11
- Microsoft Edge
- Microsoft Windows: 7, 8.1, RT 8.1, 10
- Microsoft Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Windows Server Core Installations: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Project Server 2013
- Microsoft Office Web Apps 2010
- Microsoft Office 2007, 2010, 2011, 2013, 2016
- Skype for Business 2016
- Microsoft Silverlight 5
- Microsoft SharePoint Server 2007
- Microsoft SharePoint Enterprise Server 2013, 2016

June 14 - UPDATED SYSTEMS AFFECTED:

- ***Microsoft Windows XP, Vista, 8***
- ***Microsoft Windows Server 2003***

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Microsoft Products are prone to multiple vulnerabilities, the most severe of which could allow for remote 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.

June 14 - UPDATED TECHNICAL SUMMARY:
Microsoft has released security patches for end-of-life versions of Windows that are affected by critical vulnerabilities related to the release of exploits by The Shadow Brokers.

This updated patch may not automatically appear in Windows Server Update Services for end of life systems and may require manual download. For more information on how to apply the security patches manually to End of Life systems, review the Microsoft links in the Updated References section of this advisory.

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 privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from un-trusted 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/40969d56-1b2a-e711-80db-000d3a32fc99

June 14 - UPDATED REFERENCES:
Microsoft:
https://technet.microsoft.com/en-us/library/security/4025685
https://support.microsoft.com/en-us/help/4025687/microsoft-security-advisory-4025685-guidance-for-older-platforms

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

MS-ISAC

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.