

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:

2017-063

DATE ISSUED:

07/11/2017

SUBJECT:

Critical Patches Issued for Microsoft Products, July 11, 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.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 9, 10, 11
- 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 Windows Server Core Installations: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Office Web Apps 2010
- Microsoft Office 2007, 2010, 2011, 2013, 2016
- Microsoft SharePoint Enterprise Server 2013, 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:

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.

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/f2b16606-4945-e711-80dc-000d3a32fc99>

24x7 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