



Alert – Critical Patches issued for Microsoft Products - SEPTEMBER 10, 2019

Description:

Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution. This month's security updates include patches for a total of 79 security vulnerabilities in its software, of which 17 are rated critical, 61 as important, and one moderate in severity. 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

Vulnerable or affected systems:

- Access 2010,2013,2016
- ASP.NET Core 2.1,2.2,3.0
- ChakraCore
- Edge
- Excel 2010, 2013, 2013 RT, 2016
- Exchange Server 2016, 2019
- Internet Explorer 10, 11, 9
- Lync Server 2013
- .NET Core 2.1, 2.2
- .NET Framework 3.5,3.5 AND 4.7.2,3.5 AND 4.8,4.5.2,4.6.2,4.6.2/4.7/4.7.1/4.7.2,4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2,4.7.1/4.7.2,4.7.2,4.7.2,4.7.2,4.7.1/4.7.2,4.8
- Office 2010,2013,2013 RT,2016,2019
- Office 2016 for Mac
- Office 2019 for Mac
- Office 365 ProPlus
- Project 2010, 2013, 2016
- Rome SDK 1.4.1
- SharePoint Enterprise Server 2013, 2016
- SharePoint Foundation 2010, 2013
- SharePoint Server 2019
- Visual Studio 2015 Update 3, 2017, 2017 version 15.9, 2019 version 16.0, 2019 version 16.2
- Windows 10, 10 version 1709, 7, 8.1, RT 8.1

- Windows Server (Core Installation) 2012 R2, 2012, 2016, 2019
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019
- Windows Server, version 1803 (Server Core Installation)
- Windows Server, version 1903 (Server Core Installation)
- Yammer Android

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

Solution:

Rw-CSIRT is strongly recommending **users** and **IT administrators** to:

- 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.

Affected users should: contact RW-CSIRT: Call **4045** or write to security@risa.rw to help for analyzing the source of the incident and recommendation.

The reference of a full list of all vulnerabilities can be found at the links below:

<https://portal.msrc.microsoft.com/en-us/security-guidance>
<https://portal.msrc.microsoft.com/en-us/security-guidance/summary>
<https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/24f46f0a-489c-e911-a994-000d3a33c573>

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of “early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability” and raise cyber security awareness in public.