**Alert – Critical Patches issued for Microsoft Products - May 16, 2019**

**Description:**
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.

**Vulnerable or affected systems:**

- Team Foundation Server
- Adobe Flash Player
- Microsoft Windows
- Internet Explorer
- Microsoft Edge
- Visual Studio
- Azure DevOps Server
- SQL Server
- .NET Framework
- .NET Core
- ASP .NET Core
- ChakraCore
- Online Services
- Azure
- NuGet
- Skype for Android
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows 2003
- Windows XP
- Microsoft Office and Microsoft Office Services and Web Apps
### 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.

### A full list of all vulnerabilities can be found at the link below:

- https://thehackernews.com/2019/05/microsoft-security-updates.html
- https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/e5989c8b-7046-e911-a98e-000d3a33a34d

### 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.