PTA Security Advisory-No: 53

10th, July 2019

Threat Classification: Security Vulnerabilities

Name:

- Microsoft security vulnerabilities

Source: Affect following Microsoft products:

- Microsoft Windows
- Internet Explorer
- Microsoft Edge
- Microsoft Office and Microsoft Office Services and Web Apps
- Azure DevOps
- Open Source Software
- .NET Framework
- Azure
- SQL Server
- ASP.NET
- Visual Studio
- Microsoft Exchange Server

Exploited Vulnerabilities:

CVE ID	Vulnerability	Exploitation
CVE-2019-1132	Exists when the Win32k component fails to properly handle objects in memory.	Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code in kernel mode.
CVE-2019-0880	Exists in how splwow64.exe handles certain calls	Successful exploitation of the vulnerability could allow an attacker to elevate privileges on an affected system from low-integrity to medium-integrity.
CVE-2019-1113	Exists in .NET software when the software fails to check the source markup of a file	Successful exploitation of the vulnerability could allow an attacker to run arbitrary code in the context of the current user.
CVE-2019-1072	Exists when Azure DevOps Server and Team Foundation Server (TFS) improperly handle user input	Successful exploitation of the vulnerability could allow an attacker to execute code on the target server in the context of the DevOps or TFS service account
CVE-2019-1063	Exists when Internet Explorer improperly accesses objects in memory.	Successful exploitation of the vulnerability could allow an attacker to gain the same user rights as the current user.
CVE-2019-1104	Exists in the way that Microsoft browsers access objects in memory.	Successful exploitation of the vulnerability could allow an attacker to gain the same user rights as the current user.

CVE ID	Vulnerability	Exploitation
CVE-2019-1102	Exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory.	Successful exploitation of the vulnerability could allow an attacker to take control of the affected system.
CVE-2019-1062, CVE-2019-1106, CVE-2019-1092, CVE-2019-1103, CVE-2019-1107	Exist in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge.	Successful exploitation of the vulnerabilities could allow an attacker to gain the same user rights as the current user.
CVE-2019-1004, CVE-2019-1056	Exist in the way that the scripting engine handles objects in memory in Internet Explorer.	Successful exploitation of the vulnerabilities could allow an attacker to gain the same user rights as the current user.
CVE-2019-1001	Exists in the way the scripting engine handles objects in memory in Microsoft browsers.	Successful exploitation of the vulnerability could allow an attacker to gain the same user rights as the current user.
CVE-2019-0785	Exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP failover server.	Successful exploitation of the vulnerability could allow an attacker to either run arbitrary code on the DHCP failover server or cause the DHCP service to become nonresponsive.

Recommendations:

- Use the following official patches to fix the aforementioned vulnerabilities:
  - https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/48293f19-d662-e911-a98e-000d3a33c573