Serianu cyber Security Advisory

The August 2020 Security Update

Serianu SOC Advisory Number:

TA – 2020/0013

Date(s) issued:

15th September 2020

Systems Affected:

- Microsoft Office Products

Overview:

Microsoft released security updates and non-security updates for all supported versions of the Windows operating system, client and server as well as other company products such as Microsoft Office. Security updates are also available for non-Windows products: Microsoft Edge classic and Chromium, Internet Explorer, SQL Server, Microsoft JET Database Engine, .NET Framework, ASP.NET Core, Microsoft Office, Microsoft Windows Codecs Library, Microsoft Dynamics.

The Windows updates are cumulative in nature and are provided via Windows Update, WSUS and other update management systems. This advisory covers a list of released updates and known security issues.

Adobe Patches

Adobe Reader fixed a total of 26 bugs, 8 of which came through the Zero Day Initiative (ZDI) program. Most of them were Out-of-Bounds (OOB) Reads but there were also some User-After-Free (UAF), OOB Write, stack exhaustion and memory corruption bugs addressed. One bug fixed was CVE-2020-9712. This bug could allow attackers to bypass HTML parsing mitigations within Acrobat Pro DC. Through this, an attacker can trigger the parsing of HTML documents remotely from within Acrobat.

Microsoft Patches

Microsoft released patches for 120 CVEs in Microsoft Windows, Edge (EdgeHTML-based and Chromium-based), ChakraCore, Internet Explorer (IE), Microsoft Scripting Engine, SQL Server, .NET Framework, ASP.NET

Core, Office and Office Services and Web Apps, Windows Codecs Library and Microsoft Dynamics. Of these 120 patches, 17 are listed as Critical and 103 are listed as Important in severity.

1. **CVE-2020-1380 – Scripting Engine Memory Corruption Vulnerability**

A remote code execution vulnerability that exists in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploits the vulnerability, could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could have administrative rights. An attacker could then install programs, view, change or delete data or create new accounts with full user rights.

2. **CVE-2020-1472 – NetLogon Elevation of Privilege Vulnerability**

A vulnerability in the NetLogon Remote Protocol (MS-NRPC) that could allow attackers to run their applications on a device on the network. To exploit the vulnerability, an unauthenticated attacker would use MS-NRPC to connect to a Domain Controller (DC) to obtain domain administrator access. This patch enables the DCs to protect devices. After applying this patch, users will be required to make changes to your DC.

3. **CVE-2020-1585 – Microsoft Windows Codecs Library Remote Code Execution Vulnerability**

An attacker who successfully exploits this vulnerability, could take control of the affected system. An attacker could then install programs, view, change delete data or create new accounts with full user rights. Exploitation of the vulnerability requires that a program process a specially crafted image file.

CVEs released by Microsoft for August 2020

CVE	Title	Severity
CVE-2020-1464	Windows Spoofing Vulnerability	Important
CVE-2020-1380	Scripting Engine Memory Corruption Vulnerability	Critical
CVE-2020-1046	.NET Framework Remote Code Execution Vulnerability	Critical
CVE-2020-1492	Media Foundation Memory Corruption Vulnerability	Critical
CVE-2020-1568	Microsoft Edge PDF Remote Code Execution Vulnerability	Critical
CVE-2020-1483	Microsoft Outlook Memory Corruption Vulnerability	Critical
CVE-2020-1567	MSHTML Engine Remote Code Execution Vulnerability	Critical
CVE-2020-1476	ASP.NET and .NET Elevation of Privilege Vulnerability	Important
CVE-2020-1558	Jet Database Engine Remote Code Execution Vulnerability	Important

Recommendations

Serianu recommends users to regularly update their software installations to the latest version. While staying up-to-date on Windows patches, it’s important to make sure that users update only after they have backed up important data and files.

For end users:

- Update product installations manually by choosing Help > Check for Updates.
- Automatic updates when updates are detected.
- The full Acrobat Reader installer can be downloaded from the Acrobat Reader Download Center.

For IT administrators:

- Download the enterprise installers from ftp://ftp.adobe.com/pub/adobe/, or refer to the specific release note version for links to installers.
- Install updates via your preferred methodology such as AIP-GPO, bootstrapper, SCUP/SCCM (Windows), or on macOS, Apple Remote Desktop and SSH.

Information Sharing

We encourage any organisation or individual that has access to security updates share it with us through our email: info@serianu.com.