Serianu Cyber Security Advisory

The September 2020 Security Update

Serianu SOC Advisory Number:

TA – 2020/017

Date(s) issued:

3rd November 2020

Systems Affected:

- Microsoft Office Products

Overview:

Microsoft patched 129 CVEs in September 2020 Patch Tuesday. The products for which Microsoft released security updates include: Microsoft Windows, Edge (EdgeHTML-based and Chromium-based), ChakraCore, Internet Explorer (IE), SQL Server, Office and Office Services and Web Apps, Microsoft Dynamics, Visual Studio, Exchange Server, ASP.NET, OneDrive, and Azure DevOps.

Of these 129 patches, 23 are listed as Critical while 105 are listed as Important, and 1 is listed as Moderate in severity. A total of 12 of these bugs came through the Zero Day Initiative (ZD)I program.

Adobe Patches for September 2020

Adobe released 3 patches addressing 18 unique CVEs in InDesign (page layout software), Framemaker (document processor designed for writing and editing large or complex documents,), and Adobe Experience Manager (helps you create, manage, and optimize digital customer experiences across every channel, including web, mobile apps, digital forms).

The patch for InDesign corrects 5 memory corruption bugs. The patch for Framemaker fixes an out-of-bounds read and a stack-based buffer overflow. Both are rated Critical and both were reported through the ZDI program. The patch for Experience Manager fixes a variety of bugs, but most are related to cross-site scripting (XSS). According to our research, Adobe Flash will go out of support at the end of this year 2020.

1. **CVE-2020-16875** – **Microsoft Exchange Memory Corruption Vulnerability**

CVE-2020-16875 is a memory corruption vulnerability in Microsoft Exchange Server software due to improper handling of objects in memory. Microsoft Exchange Server is Microsoft's email, calendaring, contact, scheduling and collaboration platform. To exploit this vulnerability, an attacker would simply need to send a malicious email to a vulnerable Exchange server.

Successful exploitation would allow an attacker to execute arbitrary code as SYSTEM. This level of access means an attacker would be able to perform a variety of actions, from creating new accounts on the system, to accessing, modifying or removing data, as well as installing programs.

2. **CVE-2020-1129 – Microsoft Windows Codecs Library Remote Code Execution Vulnerability**

A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system.

An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of the vulnerability requires that a program process a specially crafted image file. The update addresses the vulnerability by correcting how Microsoft Windows Codecs Library handles objects in memory.

3. **CVE-2020-0922 – Microsoft COM for Windows Remote Code Execution Vulnerability**

A remote code execution vulnerability exists in the way that Microsoft COM for Windows handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code on a target system.

To exploit the vulnerability, a user would have to open a specially crafted file or lure the target to a website hosting malicious JavaScript. The security update addresses the vulnerability by correcting how Microsoft COM for Windows handles objects in memory.

4. **CVE-2020-0951 – Windows Defender Application Control Security Feature Bypass Vulnerability**

A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement. An attacker who successfully exploited this vulnerability could execute PowerShell commands that would be blocked by WDAC.

To exploit the vulnerability, an attacker needs administrator access on a local machine where PowerShell is running. The attacker could then connect to a PowerShell session and send commands to execute arbitrary code. The update addresses the vulnerability by correcting how PowerShell commands are validated when WDAC protection is enabled.

Critical CVEs released by Microsoft for September 2020.

CVE	Title	Severity
CVE-2020-1285	GDI+ Remote Code Execution Vulnerability	Critical
CVE-2020-0878	Microsoft Browser Memory Corruption Vulnerability	Critical
CVE-2020-0922	Microsoft COM for Windows Remote Code Execution Vulnerability	Critical
CVE-2020-16862	Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability	Critical
CVE-2020-16857	Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability	Critical
CVE-2020-16875	Microsoft Exchange Memory Corruption Vulnerability	Critical
CVE-2020-1200	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-1210	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-1452	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-1453	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-1576	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-1595	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-1460	Microsoft SharePoint Server Remote Code Execution Vulnerability	Critical
CVE-2020-1129	Microsoft Windows Codecs Library Remote Code Execution Vulnerability	Critical
CVE-2020-1319	Microsoft Windows Codecs Library Remote Code Execution Vulnerability	Critical
CVE-2020-1057	Scripting Engine Memory Corruption Vulnerability	Critical
CVE-2020-1172	Scripting Engine Memory Corruption Vulnerability	Critical
CVE-2020-16874	Visual Studio Remote Code Execution Vulnerability	Critical
CVE-2020-0997	Windows Camera Codec Pack Remote Code Execution Vulnerability	Critical
CVE-2020-1508	Windows Media Audio Decoder Remote Code Execution Vulnerability	Critical
CVE-2020-1593	Windows Media Audio Decoder Remote Code Execution Vulnerability	Critical
CVE-2020-1252	Windows Remote Code Execution Vulnerability	Critical
CVE-2020-0908	Windows Text Service Module Remote Code Execution Vulnerability	Critical

Patch Management Best Practices 2020

1. **Make an inventory:** The inventory should include devices, services, and dependencies, operating systems, versions and third-party applications. Security systems such as firewalls and anti-malware programs, including their configuration and latest version.
2. **Categorize your systems:** To apply effective patch management processes, organisations need to perform a clear risk assessment to ensure the highest-risk or most sensitive parts of the infrastructure are patched first.
3. **Patching Processes** Patches to an operating system should be deployed immediately. Operating system vulnerabilities can have serious and wide-reaching effects.
4. **Deploy a test environment:** All patches should be deployed to a test environment before deploying them to the entire system.
5. **Regular Patching:** Regularly scans and auditing the systems for any vulnerabilities missed the first time around.
6. **Scanning and auditing for vulnerabilities:** Regularly scans and auditing the systems for any vulnerabilities missed the first time around.
7. **Automation:** Use an automated tool or piece of software for the patch management process.
8. **Reporting:** Undertake reporting and regular reviews to ensure that the patch management processes and software are all working as expected.

Information Sharing

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