Serianu Cyber Security Advisory

The October 2020 Security Update

Serianu SOC Advisory Number:

TA – 2020/018

Date(s) issued:

9th November 2020

Systems Affected:

- Microsoft Office Products

Overview:

Adobe Patches for October 2020

Adobe released only one patch for October 2020. The patch fixes a single vulnerability (CVE-2020-9746) for Flash Player 32.0.0.445 for Windows, macOS, Linux and Chrome OS. The patch fixes a NULL pointer Dereference bug. NULL pointer dereference issues can occur through simple programming omissions.

Successful exploitation could lead to an exploitable crash, potentially resulting in arbitrary code execution in the context of the current user. Flash player reaches its end-of-life (EOL) at the end of this year 2020.

Microsoft Patches for October 2020

Microsoft released 87 CVEs patches in October 2020 in Microsoft Windows, Office and Office Services and Web Apps, Azure Functions, Open Source Software, Exchange Server, Visual Studio, .NET Framework, Microsoft Dynamics, and the Windows Codecs Library.

Of these 87 patches, 11 are listed as Critical while 75 are listed as Important, and 1 is listed as Moderate in severity. A total of 11 of these bugs came through the Zero Day Initiative Program (ZDI) program. None of these bugs are listed as being under active attack, but six bugs are listed as publicly known at the time of release.

1. **CVE-2020-16898 – Windows TCP/IP Remote Code Execution Vulnerability**.

The bug is a critical remote code execution vulnerability in Windows 10 and Windows Server 2019 and could be exploited by sending a packet to a vulnerable machine. The remote attacker constructs a specially crafted ICMPv6 Router Advertisement packet and sends it to the remote Windows host to execute arbitrary code on the target host. TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a set of standardized rules that allow computers to communicate on a network such as the internet.

ICMPv6 (Internet Control Message Protocol) is a part of IPv6 that performs error reporting and diagnostic functions. Router Advertisements are messages generated by IPv6 routers to advertise their presence with link and Internet parameters. In this case, simply sending a specially crafted packet could lead to code execution on a vulnerable system, something which in turn could likely lead to elevated privileges.

Administrators to update any Microsoft software as soon as possible to prevent a remote compromise.

2. **CVE-2020-16947 - Microsoft Outlook Remote Code Execution Vulnerability**

A remote code execution vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the targeted user. If the targeted user is logged on with administrative user rights, an attacker 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Exploitation of the vulnerability requires that a user opens a specially crafted file with an affected version of Microsoft Outlook software. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website that contains a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, by way of an enticement in an email or instant message and then convince them to open the specially crafted file.

3. **CVE-2020-16891 - Windows Hyper-V Remote Code Execution Vulnerability**

A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. Hyper-V is a Microsoft technology that allows users to create virtual computer environments, and run and manage multiple operating systems on a single physical server. To exploit the vulnerability, an attacker could run a specially crafted application on a guest operating system that could cause the Hyper-V host operating system to execute arbitrary code. An attacker who successfully exploited the vulnerability could execute arbitrary code on the host operating system. The security update addresses the vulnerability by correcting how Hyper-V validates guest operating system user input.

4. **CVE-2020-16909 - Windows Error Reporting Elevation of Privilege Vulnerability**

The patch corrects an escalation of privilege (EoP) in the Windows Error Reporting (WER) component that could allow an authenticated attacker to execute arbitrary code with escalated privileges.

Critical CVEs released by Microsoft for October 2020.

CVE	Title	Severity
CVE-2020-17003	Base3D Remote Code Execution Vulnerability	Critical
CVE-2020-16911	GDI+ Remote Code Execution Vulnerability	Critical
CVE-2020-16915	Media Foundation Memory Corruption Vulnerability	Critical
CVE-2020-16923	Microsoft Graphics Components Remote Code Execution Vulnerability	Critical
CVE-2020-16947	Microsoft Outlook Remote Code Execution Vulnerability	Critical
CVE-2020-16951	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-16952	Microsoft SharePoint Remote Code Execution Vulnerability	Critical
CVE-2020-16967	Windows Camera Codec Pack Remote Code Execution Vulnerability	Critical
CVE-2020-16968	Windows Camera Codec Pack Remote Code Execution Vulnerability	Critical
CVE-2020-16891	Windows Hyper-V Remote Code Execution Vulnerability	Critical
CVE-2020-16898	Windows TCP/IP Remote Code Execution Vulnerability	Critical

Information Sharing

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