Ryan Buchanan

August 11, 2023

M2 Ch06 Lab Assignments: Patches and Updates Lab

RE: https://support.microsoft.com/?kbid=5028951

On August 8, 2023, a new update rolled out for Windows 10 Version 21H2 and Windows 10 Version 22H2. This update is all about improving the .NET Framework 3.5 and 4.8, which are important parts of Windows.

Now, let's talk about why this update matters. First off, it's got your back when it comes to security. It takes care of a couple of issues, like one where certain applications could sneak around security measures. This could potentially cause some trouble, so the update puts a stop to that. Another thing it does is fix a problem where unauthorized folks could mess with something called ClickOnce deployments – basically, it helps make sure that only the right people can sign and use these deployments.

Besides security stuff, the update also sorts out a few bugs. For instance, it fixes a glitch where certain documents weren't showing up properly. Plus, if you're into technical details, there are specific articles you can check out for more info.

The good news is, Microsoft hasn't spotted any new problems coming with this update. So, if you're using Windows 10 Version 21H2 or 22H2, it's a good idea to get this update on your radar and install it. It's like giving your computer a little tune-up to keep things running smoothly.

August 8, 2023-KB5028951 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H2 and Windows 10 Version 22H2

.NET

Release Date:
August 8, 2023

Version:
.NET Framework 3.5 and 4.8

The August 8, 2023 update for Windows 10 Version 21H2 and Windows 10 Version 22H2 includes security and cumulative reliability improvements in .NET Framework 3.5 and 4.8. We recommend that you apply this update as part of your regular maintenance routines. Before you install this update, see the Prerequisites and Restart requirement sections.

Summary

Security Improvements

CVE-2023-36899 - .NET Framework Remote Code Execution Vulnerability
This security update addresses a vulnerability in applications on IIS using their parent application's Application Pool which can lead to privilege escalation or other security bypasses. For more information see CVE 2023-36899.