BD FocalPoint Large Lab Server

November 2020

Critical and/or Important Security Patches for February 2016-January 2020

Microsoft® & Third-Party Patches

BD has identified patches from Microsoft® that have been identified as critical or security related for the quarter ending March 31, 2020 and including updates through January 2020. These patches were not found to adversely affect this BD product and will be applied according to customers' service agreement.

Customers that maintain patches independent of BD automated delivery should ensure the validated patches are installed on their BD systems as the acting responsible entity in order to maintain the correct security posture of the system(s).

Patch Name	Patch Description	Patch ID	Month
Service Stack Update for Windows Server 2012 R2 for x86-based Systems	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates.	4524445	November 2019
Security Update for .NET Framework 3.5 for Windows Server 2012 R2	.Net Security update	4532961	January 2020
Security Update for .NET Framework 4.5.2 for Windows Server 2012 R2	.Net Security update	4532962	January 2020
Monthly Security Quality Rollup for Windows Server 2012 R2 for x64 based Systems	This security update includes improvements and fixes that were a part of update KB4525252 (released November 19, 2019) and addresses the following issues: • Addresses an issue to support new SameSite cookie policies by default for release 80 of Google Chrome. • Security updates to the Microsoft Scripting Engine, Windows Input and Composition, Windows Media, Windows Storage and Filesystems, and Windows Server.	KB4534297	January 2020
MS16-027: Security update for Windows Server 2012 R2	The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.	KB3138910	March 2016
MS16-027: Security update for Windows Server 2012 R2	The vulnerabilities could allow remote code execution if a user opens specially	KB3138962	March 2016

	crafted media content that is hosted on a website.		
Security Only update for .NET Framework 4.5.2 for Windows Server 2012 R2	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when the .NET Framework fails to properly validate input before loading libraries	KB4014562	April 2017
Security Only update for .NET Framework 3.5 for Windows Server 2012 R2	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when the .NET Framework fails to properly validate input before loading libraries.	KB4014574	April 2017
Security Only update for .NET Framework 4.5.2 for Windows Server 2012 R2	.NET Security update	KB4506964	August 2019
Security Only update for .NET Framework 3.5 for Windows Server 2012 R2	.NET Security update	KB4506977	August 2019
Security and Quality Rollup for .NET Framework 4.5.2 for Windows Server 2012 R2	.NET Security update	KB4532927	January 2020
Security and Quality Rollup for .NET Framework 3.5 for Windows Server 2012 R2	.NET Security update	KB4532946	January 2020
MS16-019 Security update for .NET 3.5 on Windows Server 2012 R2	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.	KB3127222	February 2016
MS16-021 Security update for .NET 3.5 on Windows Server 2012 R2	The vulnerability could cause denial of service on a Network Policy Server (NPS) if an attacker sends specially crafted username strings to the NPS. This scenario could prevent RADIUS authentication on the NPS.	KB3133043	February 2016
MS16-048 Security update for Windows Server 2012 R2	The vulnerability could allow security feature bypass if an attacker logs on to a target system and runs a specially crafted application.	KB3146723	April 2016
MS16-067 Security update for Windows Server 2012 R2	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if a USB disk mounted over Remote Desktop Protocol (RDP) via Microsoft RemoteFX.	KB3155784	May 2016
MS16-072 Security update for Windows Server 2012 R2	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker launches a man-in-the-middle (MiTM) attack against the traffic passing between a domain controller and the target machine.	KB3159398	June 2016

MS16-100 Security update for Windows Server 2012 R2	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if an attacker installs an affected boot manager and bypasses Windows security features.	KB3172729	August 2016
Service Stack Update for Windows Server 2012 R2	This update fixes an issue in the Secure Boot Advanced Installer (securebootai.dll) to prevent blacklisting the boot manager in use on the system that would make the system unbootable.	KB3173424	July 2016
MS16-111 Security update for Windows Server 2012 R2	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker runs a specially crafted application on a target system.	KB3175024	September 2016
MS16-112 Security update for Windows Server 2012 R2	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if Windows improperly allows web content to load from the Windows lock screen	KB3178539	September 2016
Security Only update for .NET Framework 3.5 for Windows Server 2012 R2	This security update for the Microsoft .NET Framework resolves a security feature bypass vulnerability in which the .NET Framework (and the .NET Core) components don't completely validate certificates.	KB4014581	May 2017
Security Only update for .NET Framework 4.5.2 for Windows Server 2012 R2	This security update for the Microsoft .NET Framework resolves a security feature bypass vulnerability in which the .NET Framework (and the .NET Core) components don't completely validate certificates.	KB4014595	May 2017
Security Only update for .NET Framework 4.5.2 for Windows Server 2012 R2	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input.	KB4040958	September 2017
Security Only update for .NET Framework 3.5 for Windows Server 2012 R2	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input.	KB4040967	September 2017
Security only update for .NET Framework 4.5.2 for Windows Server 2012 R2	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input	KB4040974	November 2017

Security only update for .NET Framework 3.5 for Windows Server 2012 R2	This security update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution when Microsoft .NET Framework processes untrusted input.	KB4040981	November 2017
Security only update for .NET Framework 3.5 for Windows Server 2012 R2	This update resolves a vulnerability in Microsoft .NET Framework that could cause denial of service when .NET Framework and .NET core components process XML documents incorrectly	KB4095515	May 2018
Security only update for .NET Framework 4.5.2 for Windows Server 2012 R2	This update resolves a vulnerability in Microsoft .NET Framework that could cause denial of service when .NET Framework and .NET core components process XML documents incorrectly	KB4095517	May 2018
Security Only update for .NET Framework 4.5.2 for Windows Server 2012 R2	.NET Security update	KB4338600	August 2018
Security Only update for .NET Framework 3.5 for Windows Server 2012 R2	.NET Security update	KB4338613	August 2018
Security Only update for .NET Framework 4.5.2 for Windows Server 2012 R2	Denial of service vulnerabilities exist when .NET Framework improperly handles objects in heap memory, or when .NET Framework and .NET Core improperly process RegEx strings.	KB4495589	August 2019
Security Only update for .NET Framework 3.5 for Windows Server 2012 R2	Denial of service vulnerabilities exist when .NET Framework improperly handles objects in heap memory, or when .NET Framework and .NET Core improperly process RegEx strings.	KB4495615	August 2019
Security Only update for .NET Framework 4.5.2 for Windows Server 2012 R2	An elevation of privilege vulnerability exists when the .NET Framework common language runtime (CLR) allows file creation in arbitrary locations.	KB4514341	September 2019
Security Only update for .NET Framework 3.5 for Windows Server 2012 R2	An elevation of privilege vulnerability exists when the .NET Framework common language runtime (CLR) allows file creation in arbitrary locations.	KB4514350	September 2019
Security update for Visual Studio 2010 Service Pack 1	An information disclosure vulnerability exists if Microsoft Visual Studio incorrectly discloses arbitrary file contents if the victim opens a malicious .vscontent file.	KB4476698	January 2019
Security update for Visual Studio 2010 Service Pack 1	An information disclosure vulnerability exists if Visual Studio incorrectly discloses the contents of its memory. An attacker who exploits the vulnerability could view uninitialized memory from the computer that is used to compile a program database file	KB4091346	April 2018

Security update for Visual Studio 2010 Service Pack 1	A remote code execution vulnerability exists in Visual Studio software if the software does not check the source markup of a file for an unbuilt project.	KB4336919	July 2018

Notes

1. Service Stack update 4524445 must be installed prior to other updates listed.