BD FocalPoint Guided Screen Review Station

November 2020

Critical and/or Security Patches June 2020.

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft® that have been identified as critical or security related and include updates through June 2020.

The patches include updates that may adversely affect BD FocalPoint Guided Screen Review Station. These patches will not be and should not be installed on BD FocalPoint Guided Screen Review Station at this time.

Customers that maintain patches independent of BD automated delivery should ensure these actions are not performed as the acting responsible entity in order to maintain the correct security posture of the system(s).

| Patch Name | Patch Description | Patch ID | Month |
|---|---|---|---|
| Security Rollup for Windows 8.1 for x86-based Systems | Security updates to Windows media, Windows Shell, Windows Hyper-V, Windows datacenter networking, Windows kernel, Windows virtualization and kernel, Microsoft JET Database Engine, Windows MSXML, and Windows Server. | 4457129 | September 2018 |
| Security Rollup for Windows 8.1 for x86-based Systems | Security updates to Windows Virtualization, Windows Kernel, Windows Peripherals, the Microsoft Scripting Engine, and Windows  Server | 4530702 | December 2019 |
| Security Rollup for Windows 8.1 for x86-based Systems | • Addresses an issue to support new SameSite cookie policies by default for release 80 of Google Chrome.<br><br>• Security updates to the Microsoft Scripting Engine, Windows Input and Composition, Windows Media, Windows Storage and Filesystems, and Windows Server. | 4534297 | Jan 2020 |

**Notes**

BD FocalPoint Guided Screen Review Station

November 2020

Critical and/or Security Patches for June 2020

**Microsoft® & Third-Party Patches**

BD has identified patches from Microsoft® that have been identified as critical or security related and include updates through June 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 |
|---|---|---|---|
| Adobe Flash Security update | This security update resolves vulnerabilities in Adobe Flash Player that is installed on any of the operating systems that are listed in the "Applies to" section | 4493478 | April 2019 |
| Security Update for Windows 8.1 | Security updates to Windows Virtualization, Windows Kernel, Windows Peripherals, and Windows Server. | 4530730 | December 2019 |
| Security Update for .NET Framework 4.5.2 for Windows 8.1 | .Net Security update | 4532927 | January 2020 |
| Security Update for .NET Framework 3.5 for Windows 8.1 | A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly. An attacker who successfully exploited this vulnerability could take control of an 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. | 4532946 | February 2020 |
| Security Update for .NET Framework 3.5 for Windows 8.1 | A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly. An attacker who successfully exploited this vulnerability could take control of an 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 | 4532961 | January 2020 |

| | | | |
|---|---|---|---|
| | fewer user rights on the system could be less impacted than users who operate with administrative user rights. | | |
| Security Update for .NET Framework 4.5.2 for Windows 8.1 | A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly. An attacker who successfully exploited this vulnerability could take control of an 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. | 4532962 | January 2020 |
| Security Update for Windows 8.1 | • Addresses an issue to support new SameSite cookie policies by default for release 80 of Google Chrome.<br><br>• Security updates to Windows Input and Composition, Windows Media, Windows Storage and Filesystems, and Windows Server. | 4534309 | January 2020 |

**Notes**