# Microsoft Service Pack & Security Bulletin Support

## ReadMe

For additional information on system security, see the following link on the Avid Knowledge Base: https://kb.avid.com/articles/en_US/Troubleshooting/en239659.

### Revision History

| Date Revised | Changes Made |
|---|---|
| December 17, 2025 | December 2025 Microsoft Security Update<br><br>For details, see "Current Microsoft Security Bulletin Status" on the next page. |

## Contents

# Microsoft Security Bulletins

Install Windows Security Patches and Service Packs.

To download patches, run Windows Update.

By default Avid supports all Windows Service Packs and security patches (sometimes referred to as “hot fixes”) which apply to the environments in which Avid products are deployed. We refer to them as Windows Updates in this document.

Customers can schedule the download and installation of Windows Updates whenever they are available and make sense in their production environment. Avid tests the updates within several days of their availability. However, customers do not have to wait for the testing to be complete before installing the updates.

Our current testing methodology is to utilize Windows Update on a representative sample of Avid products upon notification of new Security Bulletin availability by Microsoft. These systems are updated and observed while under test. Once the test period has completed (approx. 5 days), support for the latest release of Security Bulletins is announced.

**Avid encourages customers to do their own independent research and to review Microsoft’s Security Update Release Notes before installing any update to your operating system. For more information, see https://portal.msrc.microsoft.com/en-us/security-guidance.**

To stay in control of potentially required reboot cycles, Avid recommends that you turn off Automatic Updates and schedule regular maintenance windows when you can update your systems, or alternatively use an automatic updating system, such as WSUS, in a controlled manner. If you deploy updates using this controlled method, you can avoid potential problems associated with automatic system restarts during main production hours.

*As mentioned, customers can take the latest Microsoft Updates before Avid’s test period is complete. There might be times when this is necessary. For example, if a threat appears quickly and the site must protect its production environment. If the Windows Update results in an issue in your production environment Avid will make best efforts to assist you in remedying the problem under current support agreements.*

# Current Microsoft Security Bulletin Status

The Microsoft security bulletins for December have been qualified with the current Avid Video, Shared Storage, and Avid Broadcast products under test. Avid reports no exceptions or issues with this month’s security updates.

For information about previous security bulletin exceptions (if any), see "Additional Information on Security Updates" on the next page. Unless explicitly called out below, all previous bulletins have passed qualification.

## Additional Information on Security Updates

This section includes information on notable security updates that were detailed in prior versions of this document.

### Notification Regarding the August 2025 Windows Updates

While not seen within Avid, Microsoft is investigating reports that some users are experiencing issues where their SSD volumes disappear or become corrupted during heavy write operations after installing KB5063878 update (August 2025). Microsoft and SSD makers are actively working on a permanent fix. Users are advised to be cautious of large file writes and consider delaying the installation of this update until the fix is released. If you believe you might be impacted by this potential situation and you have already installed the update, you might consider uninstalling KB5063878 until Microsoft determines the root cause.

### Notification Regarding the August 2024 Windows Updates

Following the release of the August updates, Microsoft discovered an issue that could cause performance issues on certain versions of Windows — including Windows Server 2019. See KB5041578 for details.

This issue was addressed in the September 2024 update with KB5043050. If you experience "system slowdowns, unresponsiveness, (or) high CPU usage", Avid recommends that you install this update to address the issue.

### Notification Regarding the June 2023 Windows Updates

After the initial qualification was completed, Avid discovered an issue with KB5028407 on a Windows Server 2016 system that caused the server to either fail to boot, or to boot into a recovery console screen. After some internal investigation, Avid concluded that the issue was related to changes related to KB5028407 and the interaction with the security endpoint system installed on that server.

Prior to enabling this update, organizations might want to contact their own security vendor to inquire about any known, related issues. If you have already installed the update and you experience any similar issues on boot, contact Microsoft Support or your security vendor for assistance.

### Notification Regarding the November 2022 Windows Updates

After the initial qualification was completed, Avid discovered an issue with KB5019959 (Windows 10) and KB5019964 (Windows Server 2016) that affects Maestro News v2022.3.x. However, it is possible that other versions of Maestro News could be affected. After installing this update, the Profile tab of the Render Manager can report the following error message:

qGetStringData: Error while fetching data ("[Microsoft][ODBC SQL Server Driver]Protocol error in TDS stream")

This issue might prevent render requests to be added to the Render Server database. If installed, Avid recommends that you uninstall KB5019959 and reboot your machine following the removal.

**Update**: After retesting, Avid can confirm that this issue has been resolved after installing updates from Microsoft. For more information, see https://learn.microsoft.com/en-us/windows/release-health/status-windows-10-1809-and-windows-server-2019#2970msgdesc.

### Notification Regarding the January 2022 Windows Updates

Although Avid did not encounter an issue with these updates, administrators should be aware that other Microsoft customers have reported problems after installing the January Monthly Rollup. These issues include unexpected Domain Controller restarts, .NET Framework errors, and others. For complete details, see the following link: https://support.microsoft.com/en-us/topic/january-11-2022-kb500624-monthly-rollup-23f4910b-6bdd-475c-bb4d-c0e961aff0bc.

### Notification Regarding the February 2020 Windows Updates

Although Avid reports no exceptions or issues with this month's security updates, Microsoft details a number of things that you need to be aware of before you consider installing KB4023057 (part of the February updates). For more information on this update, see https://support.microsoft.com/en-us/help/4023057/update-reliability-for-windows-10-versions-1507-to-1809.

### Notification Regarding the January 2020 Windows Updates

Per the following article, Microsoft has recommend that customers enable LDAP channel binding and LDAP signing for enhanced security. For more details, see https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirement-for-windows.

Following this update, Avid configured a domain controller with SSL enabled and investigated how this change might affect the following Avid products:

- **Avid NEXIS or Avid ISIS**

  Both Avid NEXIS and Avid ISIS include the features required to be compatible with this update.

  If you are already connected to an LDAP, you are not required to make any changes to your Avid storage system. All protocol decisions are handled automatically by the corresponding libraries during the connection to the LDAP system.

- **MediaCentral | Cloud UX**

  MediaCentral Cloud UX already includes the features required to be compatible with this update.

  If your system is configured without an SSL connection, you can change the respective values and redeploy the configuration. For more information, see "Configuring an Authentication Provider" in the *Avid MediaCentral | Cloud UX Installation Guide*.

- **MediaCentral | UX**

  MediaCentral UX already includes the features required to be compatible with this update.

  If your system is configured without an SSL connection, you can update the configuration through the MediaCentral UX System Settings. For more information, see "Importing Domain Users" in the *Avid MediaCentral Platform Services Installation and Configuration Guide*.

- **MediaCentral | Asset Management**

  If you are running Asset Management v2018.9 or later, users are manged through the MediaCentral Platform. As long as MediaCentral Cloud UX is configured for an SSL connection, your Asset Management system is compatible with this Microsoft update.

  If you are running a prior version of MediaCentral Asset Management (or Interplay MAM), you might need to complete the following steps to enable the SSL connection on your Asset Management server:

  - Configure your AD server port to 636
  - Add the "SecureSocketsLayer" option to the following Configuration setting: UserManagementWS/Backend/External/Ldap/AuthTypes

  

  *If the server running the user management service is not in the same domain as your Active Directory server, you must import the AD server's certificate into the Trusted Root Certification Authorities section of the Windows certificate store on your Asset Management server.*

- **MediaCentral | Newsroom Management**

  Newsroom Management and Avid iNEWS systems running RedHat or CentOS use the Kerberos authentication protocol which use encryption by default. You are not required to make any changes to the Avid systems after applying the LDAP/ADS patch.

  For more information on configuring Kerberos and working with user management, see the *Avid MediaCentral | Newsroom Management Installation Quick Guide* and the *Avid MediaCentral | Newsroom Management Setup and Configuration Guide*.

- **MediaCentral | Production Management**

  MediaCentral Production Management already includes the features required to be compatible with this update.

  If your system is configured without an SSL connection, you can update the configuration through the Interplay Administrator. For more information, see "Setting User Authentication Providers and Importing Users" in the *Avid MediaCentral | Production Management Engine Administration Guide*.

### Notification Regarding the November 2019 Windows Updates

Although Avid did not encounter an issue with these updates, administrators should be aware that other Microsoft customers have reported a problem installing the Servicing Stack Update (KB 4523208). After installing this update, the server might enter an infinite reboot loop. For additional information, see https://learn.microsoft.com/en-us/archive/msdn-technet-forums/d1a9bf15-99e9-458f-b942-e387308ad1a6.

### Notification Regarding the October 2019 Windows Updates

Although Avid reports no exceptions with this month's updates, customers should be aware that the Tamper Protection feature of Microsoft Defender is enabled by default in Windows 10 systems after completing the security updates. Tamper Protection attempts to block malicious software from making changes to Windows security features. For more information, see the following link to the Microsoft website: https://support.microsoft.com/en-us/help/4490103/windows-10-prevent-changes-to-security-settings-with-tamper-protection.

### Potential Problems with August 2019 Windows Updates:

Avid recommends that you do not install the August 13th or August 17th Windows Updates in your environment.

Microsoft customers have reported that the following components of the August 13th Windows Update have caused problems:

- KB4512488 might prevent Remote Desktop (RDP) logins on Windows Server 2012 R2.
- KB4467684 can adversely affect Cluster installations where more than 14 characters are configured for the "Minimum password length" group policy.
- The issues related to importing users from Active Directory are still present in the August 13th update. Refer to the description in "Potential Problems with August 2019 Windows Updates:" above.

For additional information on the August 13th updates see the following Microsoft support page: https://support.microsoft.com/en-us/help/4512517/windows-10-update-kb4512517

In addition, Microsoft has released a non-security related update on August 17th (KB4512495). These updates do not fix the Cluster password or AD import issues mentioned above. Avid has not tested the August 17th updates and does not recommend installing them at this time.

### Potential Problems with July 2019 Security Updates on Windows 2016 and Windows 10

Following the initial qualification, Avid was made aware of issues with KB4507459 and KB4507460. These updates alter the default trust relationship settings in domains for security reasons, and introduce a bug in Active Directory group gathering. Both issues influence the ability to import users from Active Directory for products such as MediaCentral | Cloud UX, MediaCentral | Production Management, MediaCentral | Asset Managements, and others.

Until these issues are addressed, Avid recommends that you do not install these updates in your environment. For more information on these updates, see the following Microsoft support pages:

- https://support.microsoft.com/en-us/help/4507459/windows-10-update-kb4507459
- https://support.microsoft.com/en-us/help/4507460/windows-10-update-kb4507460

### Potential Problems with May 2019 Security Updates

This set of Microsoft security updates might affect Avid customers. Specifically, customers should be aware of the following:

- An issue installing the May updates

  For more information, see https://support.microsoft.com/en-us/help/4500988/windows-update-blocked-for-windows-10-insider-program.

- An issue with Windows Defender

  For more information, see https://support.microsoft.com/en-us/help/4495666/windows-10-update-kb4495666.

- An issue with devices installed with some Asian language packs

For more information on these and other issues, see the "Known issues in this update" sections at the following links: https://support.microsoft.com/en-us/help/4494441 and https://support.microsoft.com/en-us/help/4505056

### Potential Problems with January 2019 Security Updates

It was discovered that there are potential problems with the January 2019 Microsoft Security updates. The updates in question are KB4480970 and KB4480960 which cause problems for Windows 7 SP1 and Windows 2008 R2. Customers that have Avid products installed on virtual machines that use the VMware network driver (VMXNet virtual LAN Adapter) could encounter severe network connection problems. See the following links for details:

- January 8, 2019—KB4480970 (Monthly Rollup)

  Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1

  https://support.microsoft.com/en-us/help/4480970/windows-7-update-kb4480970

- January 8, 2019—KB4480960 (Security-only update)

  Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1

  https://support.microsoft.com/en-us/help/4480960/windows-server-2008-kb4480960

The following describes the problem:

"Local users who are part of the local "Administrators" group might not be able to remotely access shares on Windows Server 2008 R2 and Windows 7 machines after installing the January 8th, 2019 security updates. This does not affect domain accounts in the local "Administrators" group."

Microsoft has released a fix for the issue: KB4487345. After installing the January updates, Avid recommends that you install KB4487345 on the following systems:

- Windows 7 Service Pack 1
- Windows Server 2008 R2 Service Pack 1

### January 2018 Security Updates

The January 2018 Microsoft updates included support for the Meltdown and Spectre vulnerabilities.

For more information on these issues, see the following page on the Avid Knowledge Base: https://kb.avid.com/articles/en_US/Troubleshooting/en239659

# Enabling Windows Updates on Avid Systems

Avid cannot guarantee the compatibility of automatic Windows Updates, or any updates to system software components. For this reason, Avid recommends that you disable Automatic Updates until Avid has approved the current month's update offerings from Microsoft.

Windows updates are often turned off on Avid servers because an unscheduled update can affect performance in a production environment. Avid recommends that you schedule regular maintenance windows where you can turn Windows Updates on and install the recommended updates. You can simplify this procedure by using a Windows Services Update Services (WSUS) server as described below.

# Using a Microsoft WSUS Server for distributing Windows Updates

By utilizing a Windows Services Update Services (WSUS) server, your Avid systems can remain off of the Internet and still get all the required updates to remain secure. Also, because you are using your own server which you control, you can ensure that the updates are qualified by Avid before you make them available to the clients. Refer to the following link for information on WSUS servers.

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852340(v=ws.11)

# Historical List of Microsoft Security Bulletin Exceptions

**MS12-078 (KB2753842)** (from late 2012) In some cases, installation of this bulletin affects the rendering of some OpenType fonts (those in OpenType Compact Font Format). A simple and effective workaround is documented in the following Avid knowledge base article:

https://kb.avid.com/articles/en_US/troubleshooting/Some-installed-Windows-fonts-are-unavailable

A link to the Microsoft Technet article follows for reference: http://support.microsoft.com/kb/2753842

**MS11-004 (KB2489256)** (from early 2011) fails to install properly on the ISIS 5000 Engine and also on the ISIS 7000 System Director on the AS3000 server only. Please do not install this update. (The affected service is IIS FTP which is enabled on the ISIS 5000 Engine and on the ISIS 7000 System Director on the AS3000 server.)

*Note also that the ISIS 7000 System Director and ISIS CIFS/FPT Server are not affected by this issue. (They do not require the MS11-004 security bulletin.) This bulletin is rated "Important" by Microsoft and we believe that customers are not exposed to undue risk.*

The patch released with Microsoft Security Advisory Notification [KB971029] was qualified in February. This patch's effect is to restrict the execution of an autorun.inf to CD and DVD media only under the Windows XP, Windows Server 2003 (x86 and x64), Windows Vista (x64) and Windows Storage Server 2008 ("R1") operating systems. (It does not affect Windows Server 2008 R2.) With this patch applied, the autorun functionality will no longer be able to be invoked from a hard drive or from USB media.

## Legal Notices



Microsoft Service Pack & Security Bulletin Support ReadMe • Revised Wednesday, December 17, 2025 • This document is distributed by Avid in online (electronic) form only, and is not available for purchase in printed form.