Microsoft recommended driver block rules

By jsuther1974

Archived: 2026-04-06 01:12:50 UTC

Microsoft has strict requirements for code running in kernel. So, malicious actors are turning to exploit vulnerabilities in legitimate and signed kernel drivers to run malware in kernel. One of the many strengths of the Windows platform is our strong collaboration with independent hardware vendors (IHVs) and OEMs. Microsoft works closely with our IHVs and security community to ensure the highest level of driver security for our customers. When vulnerabilities in drivers are found, we work with our partners to ensure they're quickly patched and rolled out to the ecosystem. The vulnerable driver blocklist is designed to help harden systems against non-Microsoft-developed drivers across the Windows ecosystem with any of the following attributes:

- Known security vulnerabilities that an attacker could exploit to elevate privileges in the Windows kernel
- Malicious behaviors (malware) or certificates used to sign malware
- Behaviors that aren't malicious but circumvent the Windows Security Model and an attacker could exploit to elevate privileges in the Windows kernel

Drivers can be submitted to Microsoft for security analysis at the Microsoft Security Intelligence Driver Submission page. For more information about driver submission, see Improve kernel security with the new Microsoft Vulnerable and Malicious Driver Reporting Center. To report an issue or request a change to the blocklist, including updating a block rule once a fixed version of a driver is available, visit the Microsoft Security Intelligence portal.

Note

Blocking drivers can cause devices or software to malfunction, and in rare cases, lead to blue screen. The vulnerable driver blocklist isn't guaranteed to block every driver found to have vulnerabilities. When we produce the blocklist, Microsoft attempts to balance the security risks from vulnerable drivers with the potential effect on compatibility and reliability. The blocklist included in this article and in the associated downloadable files usually contains a more complete set of known vulnerable drivers than the version in the OS and delivered by Windows Update. It's often necessary for us to hold back some blocks to avoid breaking existing functionality while we work with our partners who are engaging their users to update to patched versions. As always, Microsoft recommends using an explicit allowlist approach to security wherever possible, but when that isn't feasible, the use of this blocklist is a critical tool to disrupt malicious actors.

Since the Windows 11 2022 update, the vulnerable driver blocklist is enabled by default for all devices, and can be turned on or off via the Windows Security app. Except on Windows Server 2016, the vulnerable driver blocklist is also enforced when either memory integrity, also known as hypervisor-protected code integrity (HVCI), Smart App Control, or S mode is active. Users can opt in to HVCI using the Windows Security app, and HVCI is on by-default for most new Windows 11 devices.

The blocklist is updated with each new major release of Windows, typically 1-2 times per year. The most current blocklist is now also available as an optional update from Windows Update. Microsoft will occasionally publish future updates through regular Windows servicing.

Customers who always want the most up-to-date driver blocklist can also use App Control for Business to apply the latest recommended driver blocklist included in this article. For your convenience, we provide a download of the most up-to-date vulnerable driver blocklist along with instructions to apply it on your computer at the end of this article.

Microsoft recommends enabling HVCI or S mode to protect your devices against security threats. If this setting isn't possible, Microsoft recommends blocking this list of drivers within your existing App Control for Business policy. Blocking kernel drivers without sufficient testing can cause devices or software to malfunction, and in rare cases, blue screen. You should first validate this policy in audit mode and review the audit block events before deploying an enforced version.

Important

Microsoft also recommends enabling the Attack Surface Reduction (ASR) rule **Block abuse of exploited vulnerable signed drivers** to prevent an application from writing a vulnerable signed driver to disk. The ASR rule doesn't block a driver already existing on the system from loading, however enabling **Microsoft vulnerable driver blocklist** or applying this App Control policy prevents the existing driver from loading.

If you prefer to apply the vulnerable driver blocklist, follow these steps:

1. Download the App Control policy refresh tool
2. Download and extract the vulnerable driver blocklist binaries
3. Select either the audit only version or the enforced version and rename the file to SiPolicy.p7b
4. Copy SiPolicy.p7b to %windir%\system32\CodeIntegrity
5. Run the App Control policy refresh tool you downloaded in Step 1 above to activate and refresh all App Control policies on your computer

To check that the policy was successfully applied on your computer:

1. Open Event Viewer
2. Browse to **Applications and Services Logs - Microsoft - Windows - CodeIntegrity - Operational**
3. Select **Filter Current Log...**
4. Replace "<All Event IDs>" with "3099" and select OK.
5. You should find a 3099 event where the PolicyNameBuffer and PolicyIdBuffer match the Name and ID from PolicyInfo settings found in the blocklist App Control Policy XML in this article. NOTE: Your computer might have more than one 3099 event if other App Control policies are present.

Note

If any vulnerable drivers are already running that the policy would block, you must reboot your computer for those drivers to be blocked. Running processes aren't stopped when activating a new App Control policy without reboot.

The recommended blocklist xml policy file can be downloaded from the Microsoft Download Center.

This policy contains **Allow All** rules. If your version of Windows supports App Control multiple policies, we recommend deploying this policy alongside any existing App Control policies. If you do plan to merge this policy with another policy, remove the **Allow All** rules before merging it if the other policy applies an explicit allowlist. For more information, see Create an App Control Deny Policy.

Note

To use this policy with Windows Server 2016, you must convert the policy XML on a device running a newer operating system. The policies available at the Microsoft Download Center link provided earlier in this article also include versions for Windows Server 2016.

- Merge App Control for Business policies
