Improve kernel security with the new Microsoft Vulnerable and Malicious Driver Reporting Center

By Microsoft Offensive Research & Security Engineering (MORSE), Microsoft Threat Intelligence

Published: 2021-12-08 · Archived: 2026-04-06 00:05:21 UTC

Windows 10 and Windows 11 have continued to raise the security bar for drivers running in the kernel. Kernel-mode driver publishers must pass the Hardware Lab Kit (HLK) compatibility tests, malware scanning, and prove their identity through extended validation (EV) certificates. This has significantly reduced the ability for malicious actors to run nefarious kernel code on Windows 10 and Windows 11 devices.

Vulnerable driver attacks

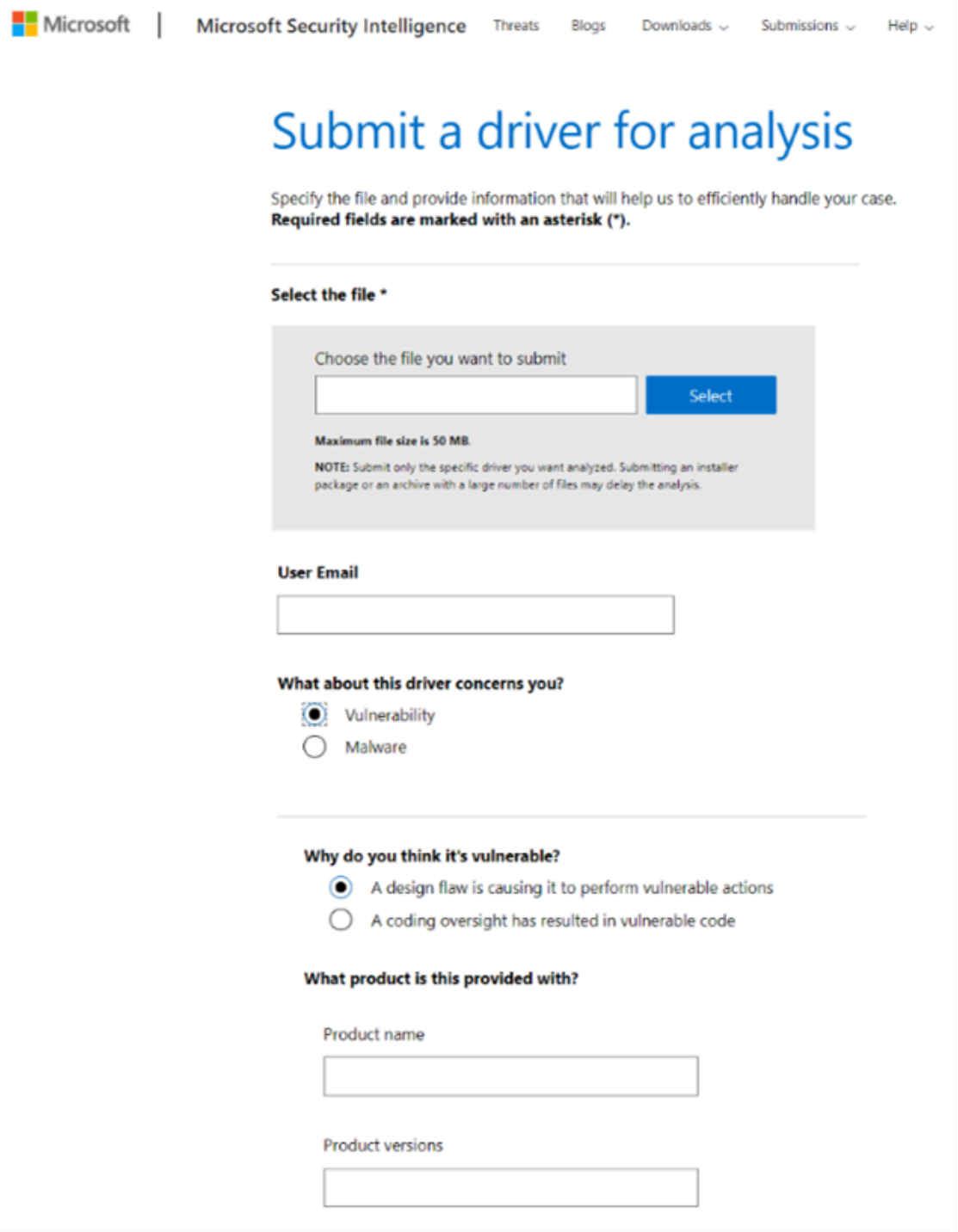
Increasingly, adversaries are leveraging legitimate drivers in the ecosystem and their security vulnerabilities to run malware. Multiple malware attacks, including RobinHood, Uroburos, Derusbi, GrayFish, and Sauron, have leveraged driver vulnerabilities (for example CVE-2008-3431,[1] CVE-2013-3956,[2] CVE-2009-0824,[3] and CVE-2010-1592).[4]

Vulnerable driver attack campaigns target security vulnerabilities in well-intentioned drivers from trusted original equipment manufacturers (OEMs) and hardware vendors to gain kernel privileges, modify kernel signing policies, and load their malicious unsigned driver into the kernel. In some cases, these unsigned drivers will disable antivirus products to avoid detection. From there, ransomware, spyware, and other types of malware can be executed.

Microsoft Defender for Endpoint and Windows Security teams work diligently with driver publishers to detect security vulnerabilities before they can be exploited by malicious software. We also build automated mechanisms to help block vulnerable versions of drivers and help protect customers against vulnerability exploits based on the ecosystem and partner engagement.

Reporting vulnerabilities: Vulnerable and Malicious Driver Reporting Center

To help protect users against these types of attacks, Microsoft has created the new Vulnerable and Malicious Driver Reporting Center. The Reporting Center is designed to be easy-to-use and requires only the driver file and a few details to open a driver analysis case. Simply provide the driver binary for our analysis, details about the vulnerability or malicious behavior of the driver, and an email address for follow-up.


Microsoft | Microsoft Security Intelligence
Threats
Blogs
Downloads
Submissions
Help
Submit a driver for analysis
Specify the file and provide information that will help us to efficiently handle your case.
Required fields are marked with an asterisk (*).
Select the file *
Choose the file you want to submit
Select
Maximum file size is 50 MB.
NOTE: Submit only the specific driver you want analyzed. Submitting an installer package or an archive with a large number of files may delay the analysis.
User Email
What about this driver concerns you?
Vulnerability
Malware
Why do you think it's vulnerable?
A design flaw is causing it to perform vulnerable actions
A coding oversight has resulted in vulnerable code
What product is this provided with?
Product name
Product versions

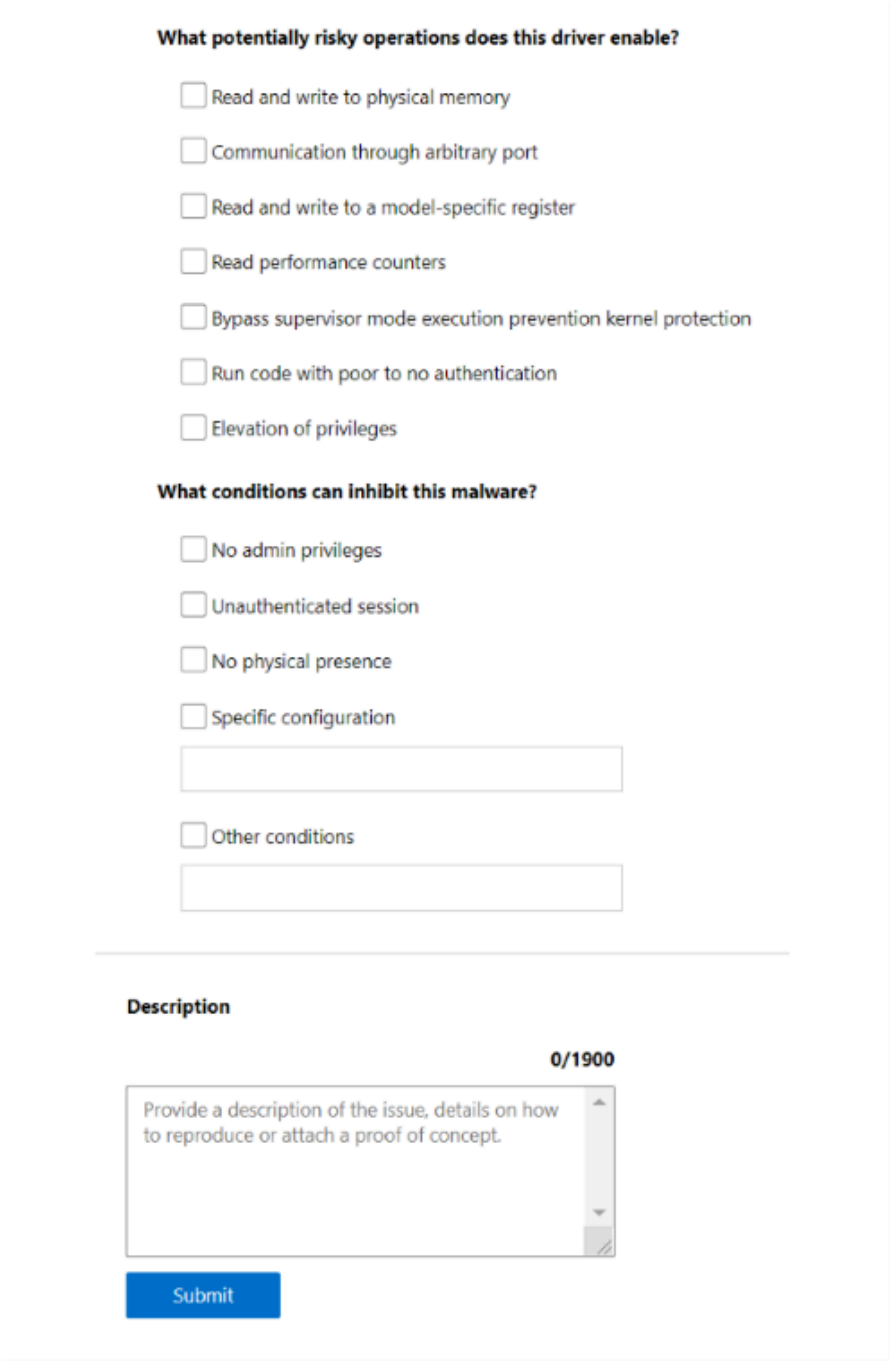


Figure 1: The Vulnerable and Malicious Driver Reporting Center.

The Reporting Center backend automatically analyzes the potentially vulnerable or malicious driver binary and identifies dangerous behaviors and security vulnerabilities including:

- Drivers with the ability to map arbitrary kernel, physical, or device memory to user mode.
- Drivers with the ability to read or write arbitrary kernel, physical, or device memory, including Port I/O and central processing unit (CPU) registers from user mode.
- Drivers that provide access to storage that bypass Windows access control.

The Reporting Center can scan and analyze Windows drivers built for x86 and x64 architectures. Vulnerable and malicious scanned drivers are flagged for analysis and investigation by Microsoft's Vulnerable Driver team. This program is currently not eligible for the Microsoft Security Response Center's Bug Bounty program.

Report a driver for analysis now.

Feedback loop: Vulnerable drivers are automatically blocked in the ecosystem

Our security teams work closely with the driver publisher to help analyze and patch the vulnerability and update in-market affected devices. Once the driver publisher patches the vulnerability, updates to all affected drivers are distributed by the driver publisher, typically through Windows Update (WU). Once affected devices receive the latest security patches, drivers with confirmed security vulnerabilities will be blocked on Windows 10 devices in the ecosystem using Microsoft Defender for Endpoint attack surface reduction (ASR) and Microsoft Windows Defender Application Control (WDAC) technologies to protect devices against exploits involving vulnerable drivers to gain access to the kernel.

Microsoft Defender for Endpoint attack surface reduction rules

Vulnerable drivers ASR rule

E3 and E5 enterprise customers will gain the benefit of using Microsoft Defender for Endpoint's ASR rules to block malicious and vulnerable drivers. ASR rules target and block entry points and code behavior used by malware and abused by attackers, preventing attacks from beginning in the first place. The vulnerable signed driver ASR rule prevents an application from writing a signed vulnerable driver to the system.

Vulnerable and malicious drivers are added to the *vulnerable driver ASR rule* to protect Microsoft Defender for Endpoint users against driver malware campaigns without any user intervention. ASR rules are supported in the following versions:

- Windows 10 Pro or Enterprise, version 1709 or later.
- Windows Server 1803 or later.
- Windows Server 2019.

Configuring the vulnerable driver ASR rule

The vulnerable driver ASR rule can be enabled and configured using Intune, mobile device management (MDM), Microsoft Endpoint Configuration Manager, Group Policy, and PowerShell. To enable the vulnerable driver ASR rule by each method, please refer to the Microsoft documentation Use attack surface reduction to prevent malware infection.

ASR rules offer the following four settings:

1. **Not configured:** Disable the ASR rule.
2. **Block:** Enable the ASR rule.
3. **Audit:** Evaluate how the ASR rule would impact your organization if enabled.
4. **Warn:** Enable the ASR rule but allow the user to bypass the block.

The vulnerable driver ASR GUID is *56a863a9-875e-4185-98a7-b882c64b5ce5*. The Intune name is *Block abuse of exploited vulnerable signed drivers*.

For the full list of ASR rule's feature differences between E3 and E5 licenses, please refer to the Microsoft documentation Attack surface reduction features across Windows versions.

Windows Defender Application Control

Microsoft driver blocklist

Driver vulnerabilities confirmed by Microsoft Defender for Endpoint and Windows Security teams, including those reported by our security community through the Vulnerable Driver Reporting Center, are blocked by the Microsoft-supplied policy. This policy is automatically updated and pushed down through WU to Secured-core devices, Hypervisor-Protected Code Integrity (HVCI) enabled, and Windows in 10 S mode devices, by default. These classes of devices use WDAC and HVCI technology to block vulnerable and malicious drivers from running on devices before they are loaded into the kernel. The vulnerable driver blocklist policy is regularly updated and pushed out through WU to help protect against the latest kernel exploits.

To learn how to turn on HVCI in Windows 10 to opt into the automated Microsoft driver blocklist, or to verify if HVCI is enabled, visit Enable virtualization-based protection of code integrity.

Defending your devices against vulnerable and malicious drivers

Creating custom WDAC block policies

Windows users can create and apply custom driver block policies to gain security parity with the Microsoft-supplied driver block policy. Microsoft publishes the block policy and recommends all customers apply kernel block rules to help prevent drivers with vulnerabilities from running on your devices or being exploited. By default, the policy is in audit mode. In this mode, drivers are not blocked from executing but will provide audit logging events. We recommend placing new policies in audit mode before enforcing them to determine the impact and scope of the blocked binaries using the audit logging events. For more information about interpreting log events, please refer to the Microsoft documentation Use audit events to create WDAC policy rules.

WDAC driver block policies are easy to create and deploy. Microsoft supplies both built-in PowerShell Cmdlets and the WDAC Wizard desktop application to create, edit, and merge WDAC policies. Below is an example of the steps to deploy the driver block policy in enforcement mode.

Step 1. Initialize the variables to be used in the script.

```
$PolicyXML = "$env:windir\schemas\CodeIntegrity\ExamplePolicies\RecommendedDriverBlock_Enforced.xml"
```

```
"$DestinationBinary=$env:windir+\System32\CodeIntegrity\SiPolicy.p7b"
```

Step 2. Run the following to convert the XML file to binary in an elevated PowerShell host.

```
ConvertFrom-CIPolicy $PolicyXML $DestinationBinary
```

Step 3. Deploy and activate the driver control policy using Windows Management Instrumentation (WMI).

```
Invoke-CimMethod -Namespace root\Microsoft\Windows\CI -
ClassName PS_UpdateAndCompareCIPolicy -MethodName Update -Arguments @{FilePath =
$DestinationBinary }
```

Learn more

For more information about deploying WDAC policies, see the Microsoft documentation Deploy WDAC policies using script.

In addition to kernel-mode block and allow rules, rules can also be created for user-mode software. See our Microsoft recommended block rules for more information. For general information about WDAC technology and policies, please see the Windows Defender Application Control official documentation.

If you are a driver developer, follow the driver security checklist and the development best practices to reduce the risk of security vulnerabilities. You can also open a driver analysis case through the new Vulnerable and Malicious Driver Reporting Center.

If you have questions about the program or suspect a driver is vulnerable or malicious, please contact vulnerabledrivers@microsoft.com.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.

---

[1]CVE-2008-3431, CVE Details. 11 October 2018.

[2]CVE-2013-3956, CVE Details. 22 August 2013.

[3]CVE-2009-0824, CVE Details. 10 October 2018.

[4]CVE-2010-1592, CVE Details. 29 April 2010.
