Recorded Future®
Sandbox

Malware Analysis Report

2025-10-25 17:30

Sample ID	251025-vzshdaylgq
Target	widevinecdm.dll
SHA256	3ed0dec36754402707c2ae4fbfa887fe3089945f6f7c1a8a3e6c1e64ad1c2648
Tags	

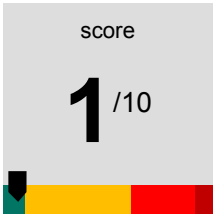
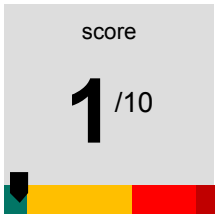


Table of Contents

Part 1. Analysis Overview



SHA256
3ed0dec36754402707c2ae4fbfa887fe3089945f6f7c1a8a3e6c1e64ad1c2648

Threat Level: No (potentially) malicious behavior was detected

The file widevinecdm.dll was found to be: No (potentially) malicious behavior was detected.

Malicious Activity Summary

N/A

Part 2. MITRE ATT&CK

N/A

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-25 17:26

3. 2. Signatures

N/A

Part 4. Analysis: behavioral2

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-25 17:25	2025-10-25 17:28	win11-20251015-en	149s	103s

4. 2. Command Line

```
rundll32.exe C:\Users\Admin\AppData\Local\Temp\widevinecdm.dll,#1
```

4. 3. Signatures

N/A

4. 4. Processes

C:\Windows\system32\rundll32.exe
```
rundll32.exe C:\Users\Admin\AppData\Local\Temp\widevinecdm.dll,#1
```

4. 5. Network

4. 6. Files

N/A

Part 5. Analysis: behavioral1

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-25 17:25	2025-10-25 17:28	win10v2004-20251016-en	149s	143s

5. 2. Command Line

```
rundll32.exe C:\Users\Admin\AppData\Local\Temp\widevinecdm.dll,#1
```

5. 3. Signatures

N/A

5. 4. Processes

C:\Windows\system32\rundll32.exe

```
rundll32.exe C:\Users\Admin\AppData\Local\Temp\widevinecdm.dll,#1
```

5. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	g.bing.com	udp
US	150.171.27.10:443	g.bing.com	tcp
US	23.33.40.152:443	www.bing.com	tcp
US	8.8.8.8:53	c.pki.goog	udp
US	142.250.81.227:80	c.pki.goog	tcp

5. 6. Files

N/A