From Patch to Exploit: Flare's Intelligence on Cybercrime After January 2026 Patch Tuesday

By Christopher Budd, Cybersecurity Evangelist

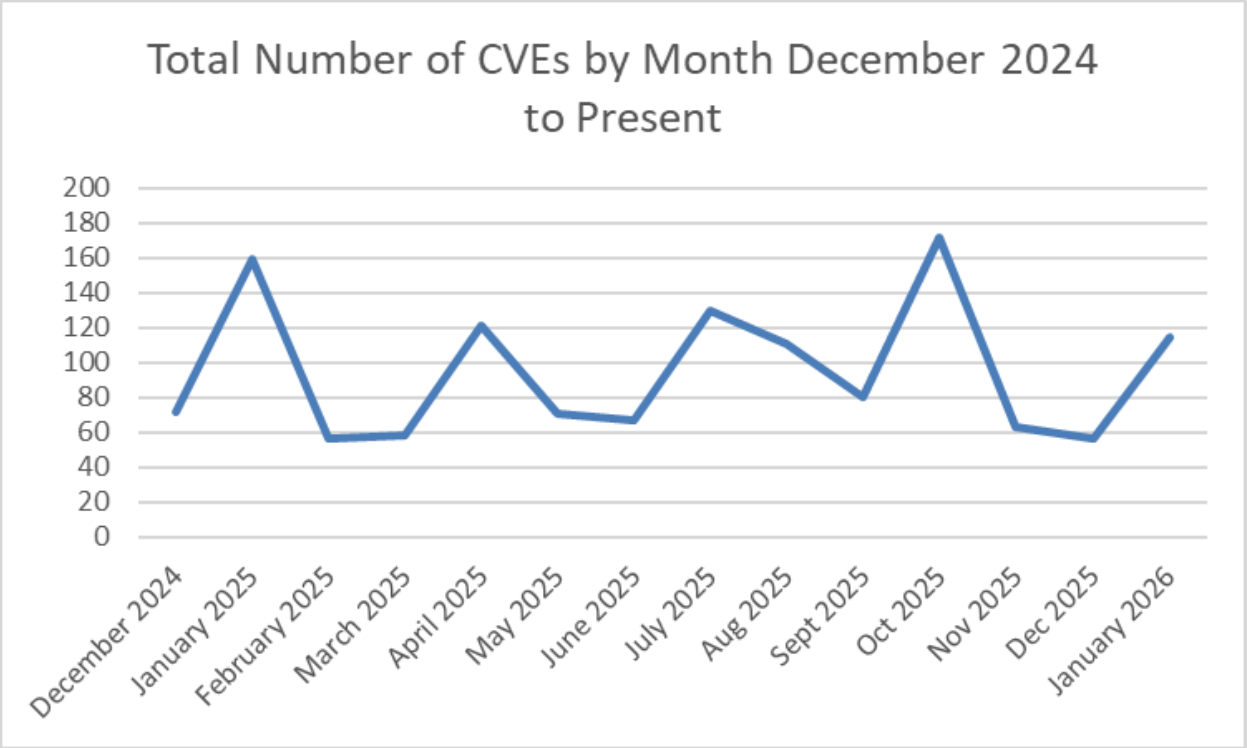
Overview

The January 2026 Patch Tuesday release is most notable for what happened AFTER patch Tuesday. Specifically, on January 26, 2026, Microsoft released CVE-2026-21509 - Microsoft Office Security Feature Bypass Vulnerability out-of-band.

As a reminder, an "out-of-band" release from Microsoft means that they view the threat environment around the vulnerability being addressed as being significant enough to warrant the risk of an out-of-process release by them and by their customers. We talk about CVE-2026-21509 in more detail below but if you haven't already deployed this patch, you should do so as quickly as possible.

Otherwise, the January release is a moderate release in terms of the number of CVEs addressed. Coming after two lighter months in November and December 2025, it's consistent with patterns of heavier months coming after lighter ones. But it's notable for not being as heavy a month as October 2025.

You can also see below that this release is not as heavy as January 2025 a year ago was.



We look at the January 2026 Patch Tuesday to highlight information of greatest importance for threat hunters and defenders focused on vulnerability management and attack prevention.

I examine the vulnerabilities that I have defined as "**notable**" using the criteria below.

I have developed these criteria based on my experience building and leading patch Tuesday for Microsoft and other companies in the industry. The criteria are the markers for vulnerabilities that are most likely to be used in attacks against unpatched systems and of greatest interest and concern for defenders.

In decreasing order of priority based on information Microsoft provided at the time of release, January 13th, 2026 and January 26, 2026 for the out-of-band fix:

1. Those that are known by Microsoft to be exploited
2. Those that are known by Microsoft to be publicly disclosed
3. Those with a "Severity Rating" of "Critical"
4. Those with an "Exploitability Assessment" of "More Likely"

For each of the vulnerabilities that meet these criteria below, I provide some information on the technology and information about the threat environment around that vulnerability as of this writing.

Vulnerabilities that are not “notable” are not covered. This is to help defenders focus on the most likely threats in this month’s release. However, remember that the threat environment changes, things that on paper appear to not be “notable” at time of release can later be under attack. Ultimately you should deploy all appropriate updates,

The information in this posting is intended to help you understand and better prioritize vulnerabilities for remediation in your environment.

In Appendix A, you will find the complete listing of this month’s Microsoft bulletins with hyperlinks to information about the individual vulnerabilities on the MSRC website.

Top Level Findings

Numbers of CVEs: Total, Critical/Important Severities, and Notable

Total CVEs this month	**115**
Total CVEs with Max Severity Critical or Important	**115**
Total CVEs with Max Severity not Critical or Important	**0**
Notable CVEs (Exploited, Publicly Disclosed, Critical, or More Likely to be Exploited)	**20**
Non-Notable CVEs	**95**

Threat Environment and Exploit Information

Exploited	**2**
Publicly Disclosed	**2**
Severity Rating of Critical	**8**
Exploitability Assessment of More Likely to Be Exploited	**9**

Vulnerability Impacts

Elevation of Privilege	**57**
Remote Code Execution	**22**
Information Disclosure	**22**
Spoofing	**5**
Security Feature Bypass	**4**

Tampering	**3**
Denial of Service	**2**

Notable CVEs

Exploited

1. CVE-2026-21509 - Microsoft Office Security Feature Bypass Vulnerability

Like we noted above, this is the top priority for January's releases, even though it was only released on January 26, 2026.

Public reports from BleepingComputer on February 2, 2026 on CVE-2026-21509 indicate that CERT-UA, the Ukrainian Computer Emergency Response Team (CERT), has observed and reported in-the-wild attacks against this vulnerability.

The vulnerability is listed as a "security feature bypass" by Microsoft. The executive summary notes that "Reliance on untrusted inputs in a security decision in Microsoft Office allows an unauthorized attacker to bypass a security feature locally. The FAQ for the vulnerability says "An attacker must send a user a malicious Office file and convince them to open it.".

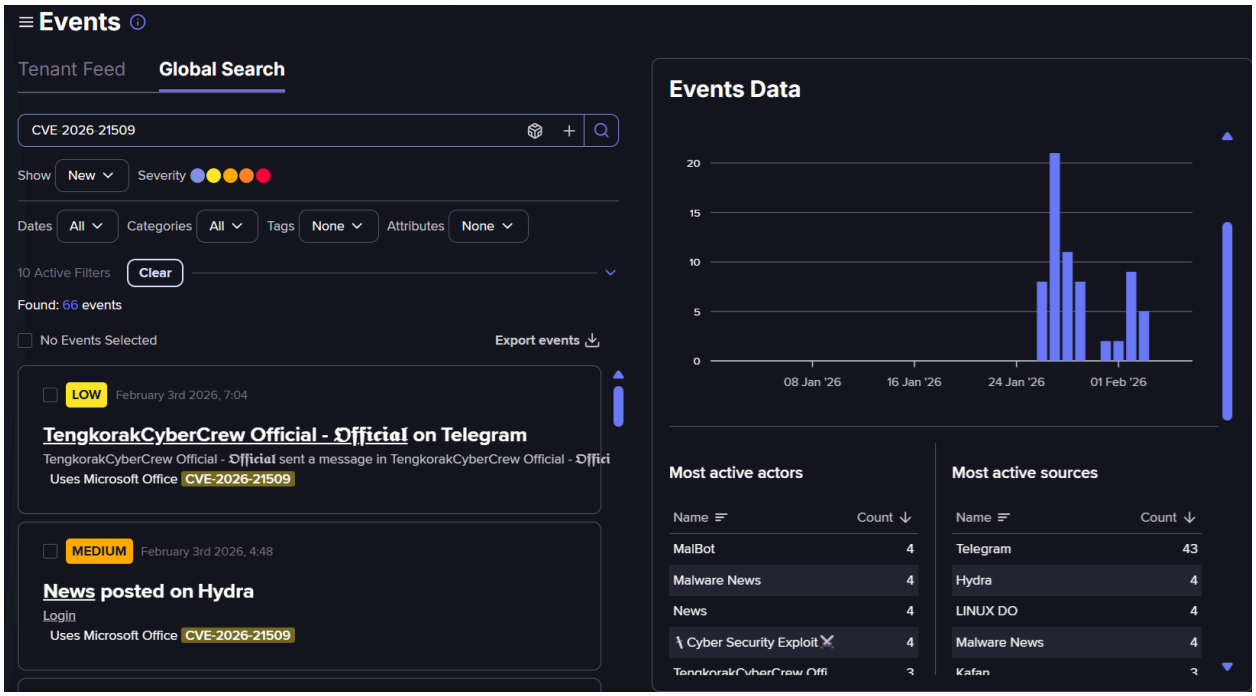
Based on the published information about the vulnerability and my time writing security bulletins like these for Microsoft, it is reasonable to postulate the attack scenario. Attackers craft Office documents designed to run malicious code and are specially malformed to suppress the security warnings normally raised when documents like this are opened as attachments. Attackers typically then send these documents as attachments in email, typically in highly targeted attacks. Once the attachment is opened and the attacker's code has executed, the attacker's malicious code is on the system and ready for the next steps in the attack. Frequently, we see tactics like this used in espionage-type attacks focused on gathering information from the targets.

The Ukrainian CERT advisory bears out this type of attack. As of this writing, no English version of the advisory is available. Claude translation cross-checked and verified with ChatGPT of the Ukrainian advisory provides the following attack chain:

1. Document opens → WebDAV connection to external resource
2. Downloads shortcut file with malicious code
3. Deploys: DLL ("EhStoreShell.dll"), shellcode image ("SplashScreen.png"), COM hijacking registry mod, scheduled task ("OneDriveHealth")
4. Terminates/restarts explorer.exe → loads DLL → executes shellcode → deploys COVENANT framework
5. C2 via legitimate Filen cloud storage (filen.io)

The Ukrainian report indicates that they've seen only a small number of attacks, what at Microsoft we would call "limited and targeted". They attribute these attacks to APT28, the group best known for their work behind the Hillary Clinton email attack in 2016.

A review of the Flare platform for information around this vulnerability shows no information about the attacks until after the release of the CERT-UA advisory and no discussions other than darkweb and Telegram news postings about the vulnerability. This is consistent with the discovery and early use of a vulnerability like this by a threat actor group like APT28.



Flare search on CVE-2026-21509 (Flare link, sign up for the free trial to access if you aren't already a customer)

While this vulnerability appears to be contained to the "limited and targeted" threat category for now, we regularly see vulnerabilities like this "trickle down" into cybercrime and more general usage quickly. As a result it makes sense to make this a top priority in your patching.

2. CVE-2026-20805 - Desktop Window Manager Information Disclosure Vulnerability

At the time of release, CVE-2026-20805 was called out at the top of the list of vulnerabilities of concern because it was the only vulnerability listed as "exploited" at that time.

The vulnerability is rated as "Important" by Microsoft, with a CVSS base score of 5.5. It's an information disclosure vulnerability and Microsoft notes in the FAQ "The type of information that could be disclosed if an attacker successfully exploited this vulnerability is a section address from a remote ALPC port which is user-mode memory."

ALPC is an "asynchronous" or “advanced” local procedure call (LPC). It’s a form of interprocess communications within the Windows platform that goes back to the earliest days.

How the vulnerability can be useful to attackers is summed up by Dustin Childs at Trend Micro’s Zero Day Initiative in his write up: “This bug allows an attacker to leak a section address from a remote ALPC port. Presumably, threat actors would then use the address in the next stage of their exploit chain – probably gaining arbitrary code execution.”

This indicates to us that this is a vulnerability that has little use on its own but can be useful as part of an attack chain, which is important information in assessing overall risk for prioritizing patches.

Another important, practical factor in prioritizing security patches is understanding the actual threat environment and how widespread exploitation or the risk of it is.

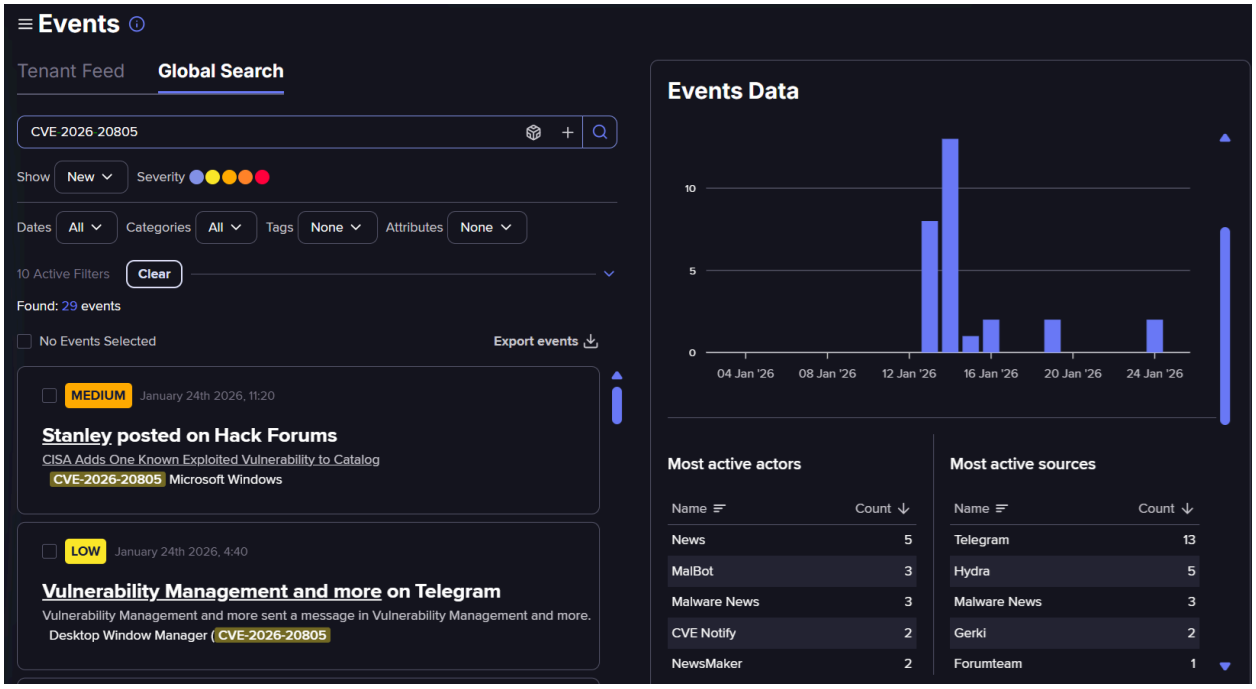
At the time of release, Microsoft noted that this vulnerability was “Exploited”. But as ZDI’s Childs notes in his write up “Microsoft offers no indication of how widespread these exploits may be, but considering the source, they are likely limited.”

One way to estimate “how widespread these exploits may be” is to look at the “Acknowledgements” for the vulnerability in the Microsoft write-up. This lists “Microsoft Threat Intelligence Center and Microsoft Security Response Center”. This tells you that while this vulnerability is publicly “exploited”, that exploitation was found by Microsoft, not someone outside of Microsoft. Microsoft does not release exploit code for vulnerabilities publicly as a matter of policy. Based on this, we can infer reasonably that public exploit information for this vulnerability at time of release was very limited, possibly known only to the attackers and Microsoft.

A search of the open web for “CVE-2026-20805 exploit” on Google, Bing, DuckDuckGo, Reddit, Mastodon (infosec.exchange instance), GitHub and Bluesky shows very little information on this vulnerability beyond announcing its release. We don’t see first hand reports of active exploits and only a couple of detailed analyses of the vulnerability by Alon Barad on CVEreports, and Penligent’s Hacking Labs.

The lack of any major indications of activity around this vulnerability on the open web gives us an indication that, as Childs notes, the exploits may indeed be limited.

Fortunately, we have the ability to augment this public information with additional intelligence from the darkweb and Telegram from Flare as shown below.



Flare search on CVE-2026-20805 (Flare link, sign up for the free trial to access if you aren't already a customer)

This shows us a spike in news postings about the vulnerability around release day, a couple of random mentions since then and nothing at all since January 24, 2026.

Taking all of the information we've outlined together, we can form a more practical threat environment assessment on our own to supplement the release day information from Microsoft.

This vulnerability was known to be exploited at time of release. But since then there is no evidence of further exploitation or movement around this vulnerability.

The vulnerability itself is rated as "Important". But it most likely can be useful only in the context of other vulnerabilities as part of a chained attack.

This gives us a more complex and nuanced picture for your risk assessment. This isn't just an "exploited at release time" vulnerability. It's an "exploited at release time with very little additional activity since then that we can find" vulnerability.

Publicly Disclosed

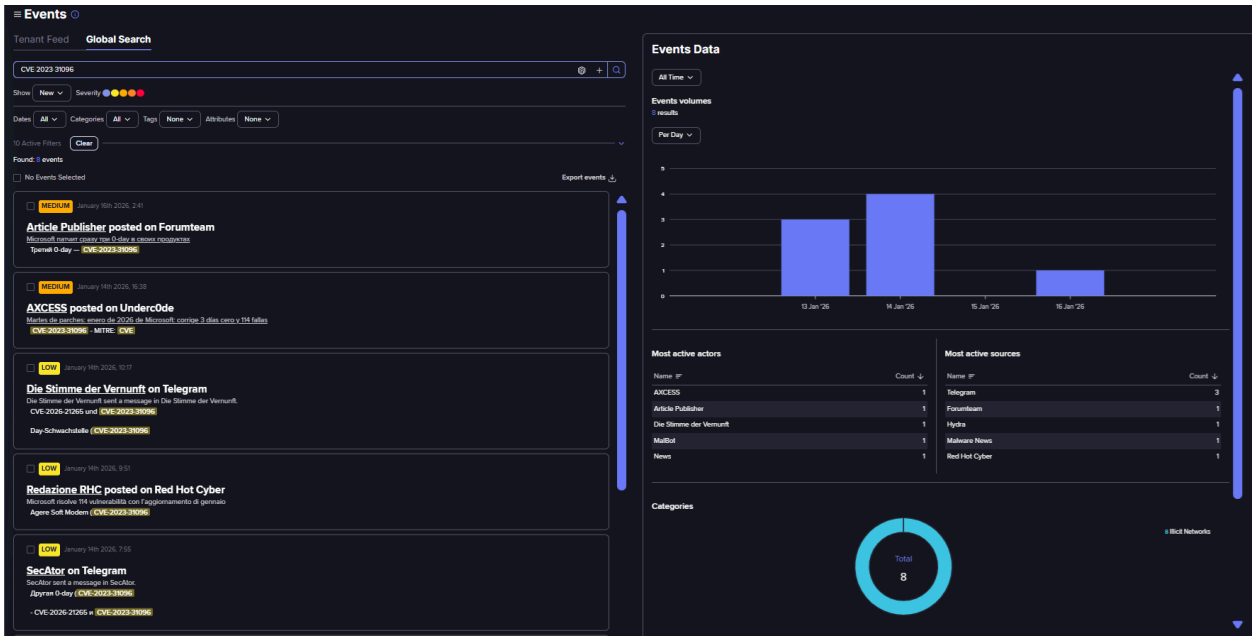
3. CVE-2023-31096 - MITRE: CVE-2023-31096 Windows Agere Soft Modem Driver Elevation of Privilege Vulnerability

This patch addresses a vulnerability that was discovered originally in 2023 affecting the Agere Soft Modem Driver that ships with Windows.

There's very little information available about this vulnerability, even after three years being in the public space.

Most importantly, there's no indication that this has ever been attacked.

A search on Flare in fact shows that throughout its lifetime, this vulnerability has only been mentioned 8 times ever throughout its history and those mentions are in the context of the January 2026 Patch Tuesday release. You can see this below where the "Event Data" is set to "All Time".



Flare search on CVE-2023-31096 (Flare link, sign up for the free trial to access if you aren't already a customer)

Even though this vulnerability is publicly known and has been for three years, you can factor this knowledge of the threat environment into your risk assessment and prioritize this appropriately.

4. CVE-2026-21265 - Secure Boot Certificate Expiration Security Feature Bypass Vulnerability

This vulnerability can be somewhat misleading in its title and labelling.

This CVE is for ensuring that the digital certificates that underpin WIndows Secure Boot are updated before they expire. If those digital certificates expire, then the Windows system's ability to receive security updates is harmed.

This issue is "public" because Microsoft has been warning about it for several months now through this knowledge base (KB) article 5062710.

This is a very important update to apply. But from a threat assessment point of view, there's almost no attack vector exposed by this.

This is backed up by a search in Flare which shows only minimal, automated mention of this vulnerability on news recaps.

Criticals

5. CVE-2026-20944 - Microsoft Word Remote Code Execution Vulnerability, CVE-2026-20952 - Microsoft Office Remote Code Execution Vulnerability, CVE-2026-20953 - Microsoft Office Remote Code Execution Vulnerability, CVE-2026-20955 - Microsoft Excel Remote Code Execution Vulnerability, CVE-2026-20957 - Microsoft Excel Remote Code Execution Vulnerability

These five critical Office vulnerabilities can be treated as a single clutch.

All five of these are memory-related vulnerabilities. They are all rated critical because of the risk of code execution from maliciously formed Office files, much like we discussed earlier in regard to CVE-2026-21509. You can also tell by how closely related they are by closeness of the CVE numbers assigned by Microsoft. Similar and related vulnerabilities are often serviced together and that can be reflected in close CVE numbers.

It is worth noting that three of the five are worth more attention because they have a preview pane attack vector. This means that they can be exploited when a malicious email message is rendered in Outlook using the preview pane with no direct interaction. The three that are affected are:

- CVE-2026-20944 - Microsoft Word Remote Code Execution Vulnerability
- CVE-2026-20952 - Microsoft Office Remote Code Execution Vulnerability
- CVE-2026-20953 - Microsoft Office Remote Code Execution Vulnerability

None of these vulnerabilities were under active attack or publicly known at the time of release. A review of Flare shows no major discussions or activity around these vulnerabilities, though it is worth noting that CVE-2026-20952 is showing up slightly more than the other four vulnerabilities.

As with all "critical" Office vulnerabilities like this, any limits on the user's account would limit the attacker's actions. If users are running as administrators, however, this presents no effective mitigation.

6. CVE-2026-20822 - Windows Graphics Component Elevation of Privilege Vulnerability

This is an elevation of privilege vulnerability that can be used by attackers to gain SYSTEM-level control. The vulnerability is the result of a race condition affecting the processing of graphics files.

One thing that's worth noting from Microsoft is "In a GPU paravirtualization scenario, an attacker who successfully exploited this vulnerability could traverse the guest's security boundary to gain access to the host environment." That makes this vulnerability of particular concern for GPU paravirtualization scenarios.

It's worth noting that while "critical" in severity, this vulnerability is assessed as "exploitation less likely".

There is minimal mention of this vulnerability in Flare.

7. CVE-2026-20854 - Windows Local Security Authority Subsystem Service (LSASS) Remote Code Execution Vulnerability

This vulnerability can enable an attacker to execute code locally in the SYSTEM-level security context. It occurs as a result of a use after free condition within the Local Security Authority Subsystem Service (LSASS).

It's worth noting that this also is rated as "critical" but also with "exploitation less likely".

There is minimal mention of this vulnerability in Flare.

8. CVE-2026-20876 - Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability

This is another local vulnerability: an attacker would have to run code on the vulnerable system to exploit this vulnerability. This is also an elevation of privilege (EoP) vulnerability, meaning that an attacker could use it to elevate to administrative privileges, making it more likely to be used in conjunction with other vulnerabilities rather than alone.

It's also worth noting that this too is rated as "critical" but also with "exploitation less likely". And once again, there is minimal mention of this vulnerability in Flare.

Exploitability More Likely

9. CVE-2026-20922 - Windows NTFS Remote Code Execution Vulnerability, CVE-2026-20840 - Windows NTFS Remote Code Execution Vulnerability
10. CVE-2026-20843 - Windows Routing and Remote Access Service (RRAS) Elevation of Privilege Vulnerability
11. CVE-2026-20871 - Desktop Windows Manager Elevation of Privilege Vulnerability
12. CVE-2026-20860 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
13. CVE-2026-20820 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
14. CVE-2026-20817- Windows Error Reporting Service Elevation of Privilege Vulnerability
15. CVE-2026-20816 - Windows Installer Elevation of Privilege Vulnerability

This month there are eight “Important” and “Exploitation More Likely” vulnerabilities that are not “exploited” or “publicly disclosed” . All eight affect Microsoft Windows. Two of these vulnerabilities are remote code execution and the remaining six are elevation of privilege (EoP).

For those interested in more details on the code execution vulnerabilities which both affect Windows NTFS, Pietro Melillo has a good write up which also includes information on how attackers could seek to exploit these vulnerabilities.

Beyond that write up, however, there is no more movement towards exploits or attack code against any of these.

Multiple Vulnerability Clusters

Often it is helpful to see when similar vulnerabilities being addressed occur around specific products, technologies or features. The below table shows this month’s occurrences of multiple vulnerability clusters.

Windows Management Services Elevation of Privilege Vulnerability	**11**
Windows SMB Server Elevation of Privilege Vulnerability	**5**
Microsoft Excel Remote Code Execution Vulnerability	**5**
Windows File Explorer Information Disclosure Vulnerability	**4**

Win32k Elevation of Privilege Vulnerability	**3**
Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	**3**
Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	**3**
Windows Virtualization-Based Security (VBS) Information Disclosure Vulnerability	**2**
Microsoft Office Remote Code Execution Vulnerability	**2**
Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability	**2**
Microsoft Word Remote Code Execution Vulnerability	**2**
Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	**2**
Windows NTFS Remote Code Execution Vulnerability	**2**
Windows Hello Tampering Vulnerability	**2**
Capability Access Management Service (camsvc) Information Disclosure Vulnerability	**2**
DirectX Graphics Kernel Elevation of Privilege Vulnerability	**2**
Tablet Windows User Interface (TWINUI) Subsystem Information Disclosure Vulnerability	**2**
Microsoft SharePoint Server Remote Code Execution Vulnerability	**2**
NTLM Hash Disclosure Spoofing Vulnerability	**2**
Windows Kernel Information Disclosure Vulnerability	**2**

Appendix A: January 2026 Microsoft CVEs

Below is the complete list of CVEs released this month. This data is taken from the Microsoft Security Response Center (MSRC) Security Update Guide and contains all CVEs that were released on January 13, 2026 and the out-of-band fix from January 26, 2026. It does not contain any third-party or Chromium (Microsoft Edge) vulnerabilities.

The data below has been grouped and sorted as follows:

- All where Exploited = Yes
- All where Publicly Disclosed = Yes
- All where Severity = Critical
- All where Exploitation = More Likely, sorted by decreasing severity, sorted alphabetically by impact
- All where Exploitation = Less Likely, sorted by decreasing severity, sorted alphabetically by impact
- All where Exploitation = Unlikely, sorted by decreasing severity, sorted alphabetically by impact
- Any remaining items

Exploited = Yes	**2**						
Release date	**CVE Number**	**CVE Title**	**Publicly disclosed**	**Exploitability assessment**	**Exploited**	**Impact**	**Max Severity**
Jan 13, 2026	CVE-2026-20805	Desktop Window Manager Information Disclosure Vulnerability	No	Exploitation Detected	Yes	Information Disclosure	Important
Jan 26, 2026	CVE-2026-21509	Microsoft Office Security Feature Bypass Vulnerability	No	Exploitation Detected	Yes	Security Feature Bypass	Important
Publicly Disclosed = Yes	**2**						
Release date	**CVE Number**	**CVE Title**	**Publicly disclosed**	**Exploitability assessment**	**Exploited**	**Impact**	**Max Severity**
Jan 13, 2026	CVE-2023-31096	MITRE: CVE-2023-31096 Windows Agere Soft Modem Driver Elevation of Privilege Vulnerability	Yes	Exploitation More Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-21265	Secure Boot Certificate Expiration Security Feature Bypass Vulnerability	Yes	Exploitation Less Likely	No	Security Feature Bypass	Important
Max Severity = Critical	**8**						
Release date	**CVE Number**	**CVE Title**	**Publicly disclosed**	**Exploitability assessment**	**Exploited**	**Impact**	**Max Severity**

Jan 13, 2026	CVE-2026-20957	Microsoft Excel Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Critical
Jan 13, 2026	CVE-2026-20955	Microsoft Excel Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Critical
Jan 13, 2026	CVE-2026-20952	Microsoft Office Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Critical
Jan 13, 2026	CVE-2026-20953	Microsoft Office Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Critical
Jan 13, 2026	CVE-2026-20944	Microsoft Word Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Critical
Jan 13, 2026	CVE-2026-20822	Windows Graphics Component Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Critical
Jan 13, 2026	CVE-2026-20854	Windows Local Security Authority Subsystem Service (LSASS) Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Critical
Jan 13, 2026	CVE-2026-20876	Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Critical
Exploitability = More Likely	**8**						

Release date	CVE Number	CVE Title	Publicly disclosed	Exploitability assessment	Exploited	Impact	Max Severity
Jan 13, 2026	CVE-2026-20871	Desktop Windows Manager Elevation of Privilege Vulnerability	No	Exploitation More Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20860	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	No	Exploitation More Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20820	Windows Common Log File System Driver Elevation of Privilege Vulnerability	No	Exploitation More Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20817	Windows Error Reporting Service Elevation of Privilege Vulnerability	No	Exploitation More Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20816	Windows Installer Elevation of Privilege Vulnerability	No	Exploitation More Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20843	Windows Routing and Remote Access Service (RRAS) Elevation of Privilege Vulnerability	No	Exploitation More Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20922	Windows NTFS Remote Code Execution Vulnerability	No	Exploitation More Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20840	Windows NTFS Remote Code Execution Vulnerability	No	Exploitation More Likely	No	Remote Code Execution	Important
Exploitability = Less Likely	**62**						

Release date	CVE Number	CVE Title	Publicly disclosed	Exploitability assessment	Exploited	Impact	Max Severity
Jan 13, 2026	CVE-2026-20875	Windows Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability	No	Exploitation Less Likely	No	Denial of Service	Important
Jan 13, 2026	CVE-2026-21224	Azure Connected Machine Agent Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20815	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20836	DirectX Graphics Kernel Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20814	DirectX Graphics Kernel Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20941	Host Process for Windows Tasks Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20842	Microsoft DWM Core Library Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20803	Microsoft SQL Server Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20826	Tablet Windows User Interface (TWINUI) Subsystem Information	No	Exploitation Less Likely	No	Elevation of Privilege	Important

		Disclosure Vulnerability					
Jan 13, 2026	CVE-2026-20863	Win32k Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20811	Win32k Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20965	Windows Admin Center Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20831	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20810	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20844	Windows Clipboard Server Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20808	Windows File Explorer Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20809	Windows Kernel Memory Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20859	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important

Jan 13, 2026	CVE-2026-20869	Windows Local Session Manager (LSM) Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20874	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20873	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20866	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20861	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20924	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20923	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20877	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20865	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20858	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important

Jan 13, 2026	CVE-2026-20832	Windows Remote Procedure Call Interface Definition Language (IDL) Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20938	Windows Virtualization-Based Security (VBS) Enclave Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20853	Windows WalletService Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20870	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	No	Exploitation Less Likely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20851	Capability Access Management Service (camsvc) Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20835	Capability Access Management Service (camsvc) Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20962	Dynamic Root of Trust for Measurement (DRTM) Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20958	Microsoft SharePoint Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-	TPM Trustlet Information	No	Exploitation Less Likely	No	Information	Important

	20829	Disclosure Vulnerability				Disclosure	
Jan 13, 2026	CVE-2026-20825	Windows Hyper-V Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20833	Windows Kerberos Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20838	Windows Kernel Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20935	Windows Virtualization-Based Security (VBS) Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20819	Windows Virtualization-Based Security (VBS) Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20828	Windows rndismp6.sys Information Disclosure Vulnerability	No	Exploitation Less Likely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-21226	Azure Core shared client library for Python Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20950	Microsoft Excel Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important

Jan 13, 2026	CVE-2026-20956	Microsoft Excel Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20946	Microsoft Excel Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20943	Microsoft Office Click-To-Run Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20963	Microsoft SharePoint Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20951	Microsoft SharePoint Server Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20948	Microsoft Word Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20837	Windows Media Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20868	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20856	Windows Server Update Service (WSUS) Remote Code Execution Vulnerability	No	Exploitation Less Likely	No	Remote Code Execution	Important

Jan 13, 2026	CVE-2026-20949	Microsoft Excel Security Feature Bypass Vulnerability	No	Exploitation Less Likely	No	Security Feature Bypass	Important
Jan 13, 2026	CVE-2026-20824	Windows Remote Assistance Security Feature Bypass Vulnerability	No	Exploitation Less Likely	No	Security Feature Bypass	Important
Jan 13, 2026	CVE-2026-20959	Microsoft SharePoint Server Spoofing Vulnerability	No	Exploitation Less Likely	No	Spoofing	Important
Jan 13, 2026	CVE-2026-20872	NTLM Hash Disclosure Spoofing Vulnerability	No	Exploitation Less Likely	No	Spoofing	Important
Jan 13, 2026	CVE-2026-20925	NTLM Hash Disclosure Spoofing Vulnerability	No	Exploitation Less Likely	No	Spoofing	Important
Jan 13, 2026	CVE-2026-20834	Windows Spoofing Vulnerability	No	Exploitation Less Likely	No	Spoofing	Important
Jan 13, 2026	CVE-2026-20812	LDAP Tampering Vulnerability	No	Exploitation Less Likely	No	Tampering	Important
Jan 13, 2026	CVE-2026-20852	Windows Hello Tampering Vulnerability	No	Exploitation Less Likely	No	Tampering	Important
Exploitability = Unlikely	**33**						
Release date	**CVE Number**	**CVE Title**	**Publicly disclosed**	**Exploitability assessment**	**Exploited**	**Impact**	**Max Severity**

Jan 13, 2026	CVE-2026-20927	Windows SMB Server Denial of Service Vulnerability	No	Exploitation Unlikely	No	Denial of Service	Important
Jan 13, 2026	CVE-2026-21221	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20830	Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20920	Win32k Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20940	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20857	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20864	Windows Connected Devices Platform Service Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20929	Windows HTTP.sys Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20849	Windows Kerberos Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20867	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important

Jan 13, 2026	CVE-2026-20918	Windows Management Services Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2024-55414	Windows Motorola Soft Modem Driver Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20848	Windows SMB Server Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20934	Windows SMB Server Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20926	Windows SMB Server Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20921	Windows SMB Server Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20919	Windows SMB Server Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20931	Windows Telephony Service Elevation of Privilege Vulnerability	No	Exploitation Unlikely	No	Elevation of Privilege	Important
Jan 13, 2026	CVE-2026-20821	Remote Procedure Call Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20827	Tablet Windows User Interface (TWINUI) Subsystem Information	No	Exploitation Unlikely	No	Information Disclosure	Important

		Disclosure Vulnerability					
Jan 13, 2026	CVE-2026-20839	Windows Client-Side Caching (CSC) Service Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20939	Windows File Explorer Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20937	Windows File Explorer Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20932	Windows File Explorer Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20823	Windows File Explorer Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20818	Windows Kernel Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20862	Windows Management Services Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-20936	Windows NDIS Information Disclosure Vulnerability	No	Exploitation Unlikely	No	Information Disclosure	Important
Jan 13, 2026	CVE-2026-21219	Inbox COM Objects (Global Memory) Remote Code Execution Vulnerability	No	Exploitation Unlikely	No	Remote Code Execution	Important

Jan 13, 2026	CVE-2026-20947	Microsoft SharePoint Server Remote Code Execution Vulnerability	No	Exploitation Unlikely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-0386	Windows Deployment Services Remote Code Execution Vulnerability	No	Exploitation Unlikely	No	Remote Code Execution	Important
Jan 13, 2026	CVE-2026-20847	Microsoft Windows File Explorer Spoofing Vulnerability	No	Exploitation Unlikely	No	Spoofing	Important
Jan 13, 2026	CVE-2026-20804	Windows Hello Tampering Vulnerability	No	Exploitation Unlikely	No	Tampering	Important

Monitor for Emerging Threats with Flare

Flare helps security practitioners stay ahead of newly disclosed CVEs by continuously monitoring the clear and dark web and threat actor communities for early signals of exploitation. Flare's collection includes more than 50,000 cybercrime Telegram channels, hundreds of cybercrime forums, ransomware leak sites, and dark web marketplaces, in addition to one of the most comprehensive sets of breached identity data in the industry.
See what external threats are exposed for your organization by signing up for our free trial.