Exploitation of CLFS zero-day leads to ransomware activity

microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/

By Microsoft Threat Intelligence April 8, 2025

Microsoft Threat Intelligence Center (MSTIC) and Microsoft Security Response Center (MSRC) have discovered post-compromise exploitation of a zero-day elevation of privilege vulnerability in the Windows Common Log File System (CLFS) against a small number of targets. The targets include organizations in the information technology (IT) and real estate sectors of the United States, the financial sector in Venezuela, a Spanish software company, and the retail sector in Saudi Arabia. Microsoft released security updates to address the vulnerability, tracked as CVE-2025-29824, on April 8, 2025.

In addition to discovering the vulnerability, Microsoft also found that the exploit has been deployed by PipeMagic malware. Microsoft is attributing the exploitation activity to Storm-2460, which also used PipeMagic to deploy ransomware. Ransomware threat actors value post-compromise elevation of privilege exploits because these could enable them to escalate initial access, including handoffs from commodity malware distributors, into privileged access. They then use privileged access for widespread deployment and detonation of ransomware within an environment. Microsoft highly recommends that organizations prioritize applying security updates for elevation of privilege vulnerabilities to add a layer of defense against ransomware attacks if threat actors are able to gain an initial foothold.

This blog details Microsoft's analysis of the observed CLFS exploit and related activity targeting our customers. This information is shared with our customers and industry partners to improve detection of these attacks and encourage rapid patching or other mitigations, as appropriate. A more comprehensive recommendations section, with indicators of compromise and detection details can be found at the end of the blog post.

CVE 2025-29824: A zero-day vulnerability in the Common Log File System (CLFS)

The exploit activity discovered by Microsoft targets a zero-day vulnerability in the Common Log File System (CLFS) kernel driver. Successful exploitation allows an attacker running as a standard user account to escalate privileges. The vulnerability is tracked as CVE-2025-29824 and was fixed on April 8, 2025.

Pre-exploitation activity

While Microsoft hasn't determined the initial access vectors that led to the devices being compromised, there are some notable pre-exploitation behaviors by Storm-2460. In multiple cases, the threat actor used the certutil utility to download a file from a legitimate third-party website that was previously compromised to host the threat actor's malware.

The downloaded file was a malicious MSBuild file, a technique described here, that carried an encrypted malware payload. Once the payload was decrypted and executed via the *EnumCalendarInfoA* API callback, the malware was found to be PipeMagic, which Kaspersky documented in October 2024. Researchers at ESET have also observed the use of PipeMagic in 2023 in connection with the deployment of a zero-day exploit for a Win32k vulnerability assigned CVE-2025-24983. A domain used by the PipeMagic sample was *aaaaabbbbbbb.eastus.cloudapp.azure[.]com,* which has now been disabled by Microsoft.

CLFS exploit activity

Following PipeMagic deployment, the attackers launched the CLFS exploit in memory from a *dllhost.exe* process.

The exploit targets a vulnerability in the CLFS kernel driver. It's notable that the exploit first uses the *NtQuerySystemInformation* API to leak kernel addresses to user mode. However, beginning in Windows 11, version 24H2, access to certain System Information Classes within *NtQuerySystemInformation* became available only to users with *SeDebugPrivilege*, which typically only admin-like users can obtain. This meant that the exploit did not work on Windows 11, version 24H2, even if the vulnerability was present.

The exploit then utilizes a memory corruption and the *RtlSetAllBits* API to overwrite the exploit process's token with the value 0xFFFFFFFF, enabling all privileges for the process, which allows for process injection into SYSTEM processes.

As part of the exploitation, a CLFS BLF file with the following path is created by the exploit's *dllhost.exe* process: *C:\ProgramData\SkyPDF\PDUDrv.blf*.

Post-exploitation activity leads to ransomware activity

Upon successful exploitation, a payload is injected into *winlogon.exe.* This payload then injected the Sysinternals *procdump.exe* tool into another *dllhost.exe* and ran it with the following command line:

```
C:\Windows\system32\dllhost.exe -accepteula -r -ma lsass.exe c:\programdata\[random letters].
```

Having done this, the actor was able to dump the memory of LSASS and parse it to obtain user credentials.

Then, Microsoft observed ransomware activity on target systems. Files were encrypted and a random extension added, and a ransom note with the name *!_READ_ME_REXX2_!.txt* was dropped. Microsoft is tracking activity associated with this ransomware as Storm-2460.

Although we weren't able to obtain a sample of ransomware for analysis, we're including some notable events surrounding the activity to better help defenders:

- Two .onion domains have been seen in the *!_READ_ME_REXX2_!.txt* ransom notes
  jbdg4buq6jd7ed3rd6cynqtq5abttuekjnxqrqyvk4xam5i7ld33jvqd.onion which has been tied to the RansomEXX ransomware family
  uyhi3ypdkfeymyf5v35pbk3pz7st3zamsbjzf47jiqbcm3zmikpwf3qd.onion
- The ransomware is launched from *dllhost.exe* with the command line:

```
--do [path_to_ransom] (for example, C:\Windows\system32\dllhost.exe --do C:\foobar)
```

- The file extension on the encrypted files is random per device, but the same for every file
- Some typical ransomware commands that make recovery or analysis harder are executed, including:
  bcdedit /set {default} recoveryenabled no
  wbadmin delete catalog -quiet
  wevtutil cl Application
- In one observed case the actor spawned *notepad.exe* as SYSTEM

Mitigation and protection guidance

Microsoft released security updates to address CVE 2025-29824 on April 8, 2025. Customers running Windows 11, version 24H2 are not affected by the observed exploitation, even if the vulnerability was present. Microsoft urges customers to apply these updates as soon as possible.

Microsoft recommends the following mitigations to reduce the impact of activity associated with Storm-2460:

- Refer to our blog Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself for robust measures to defend against ransomware.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a majority of new and unknown variants.
- Use device discovery to increase your visibility into your network by finding unmanaged devices on your network and onboarding them to Microsoft Defender for Endpoint. Ransomware attackers often identify unmanaged or legacy systems and use these blind spots to stage attacks.
- Run EDR in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume. Use Microsoft Defender Vulnerability Management to assess your current status and deploy any updates that might have been missed.
- Microsoft 365 Defender customers can turn on attack surface reduction rules to prevent common attack techniques used in ransomware attacks:
- Use advanced protection against ransomware

Microsoft Defender XDR detections

Microsoft Defender XDR customers can refer to the list of applicable detections below. Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threats associated with this activity as the following malware:

- SilverBasket (Win64/Windows)
- MSBuildInlineTaskLoader.C (Script/Windows)
- SuspClfsAccess (Win32/Windows)

Microsoft Defender for Endpoint

The following alerts might indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity.

- A process was injected with potentially malicious code
- Potential Windows DLL process injection
- Suspicious access to LSASS service
- Sensitive credential memory read
- Suspicious process injection observed
- File backups were deleted
- Ransomware behavior detected in the file system

Microsoft Security Copilot

Security Copilot customers can use the standalone experience to create their own prompts or run the following pre-built promptbooks to automate incident response or investigation tasks related to this threat:

- Incident investigation
- Microsoft User analysis
- Threat actor profile
- Threat Intelligence 360 report based on MDTI article
- Vulnerability impact assessment

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

Hunting queries

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

Search for devices having CVE-2025-29814 exposure

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2025-29814")
| project
DeviceId,DeviceName,OSPlatform,OSVersion,SoftwareVendor,SoftwareName,SoftwareVersion,
CveId,VulnerabilitySeverityLevel
| join kind=inner ( DeviceTvmSoftwareVulnerabilitiesKB | project CveId,
CvssScore,IsExploitAvailable,VulnerabilitySeverityLevel,PublishedDate,VulnerabilityDes
 ) on CveId
| project
DeviceId,DeviceName,OSPlatform,OSVersion,SoftwareVendor,SoftwareName,SoftwareVersion,
CveId,VulnerabilitySeverityLevel,CvssScore,IsExploitAvailable,PublishedDate,Vulnerabil
```

Detect CLFS BLF file creation after exploitation of CVE 2025-29824

```
DeviceFileEvents
| where FolderPath has "C:\\ProgramData\\SkyPDF\\" and FileName endswith ".blf"
```

LSSASS process dumping activity

```
SecurityEvent
  | where EventID == 4688
  | where CommandLine has("dllhost.exe -accepteula -r -ma lsass.exe")
  | extend timestamp = TimeGenerated, AccountCustomEntity = Account, HostCustomEntity
= Computer
```

Ransomware process activity

```
let cmdlines = dynamic(["C:\\Windows\\system32\\dllhost.exe --do","bcdedit /set
{default} recoveryenabled no","wbadmin delete catalog -quiet","wevtutil cl
Application"]);
DeviceProcessEvents
| where ProcessCommandLine has_any (cmdlines)
| project TimeGenerated, DeviceName, ProcessCommandLine, AccountDomain, AccountName
```

PipeMagic and RansomEXX fansomware domains

```
let domains =
dynamic(["aaaaabbbbbbb.eastus.cloudapp.azure.com","jbdg4buq6jd7ed3rd6cynqtq5abttuekjnx

DeviceNetworkEvents
| where RemoteUrl has_any (domains)
| project TimeGenerated, DeviceId, DeviceName, Protocol, LocalIP, LocalIPType,
LocalPort,RemoteIP, RemoteIPType, RemotePort, RemoteUrl
```

Indicators of compromise

Indicator	Type	Description
C:\ProgramData\SkyPDF\PDUDrv.blf	Path	Dropped during CLFS exploit
C:\Windows\system32\dllhost.exe –do	Command line	Injected dllhost
bcdedit /set {default} recoveryenabled no	Command line	Ransomware command
wbadmin delete catalog -quiet	Command line	Ransomware command
wevtutil cl Application	Command line	Ransomware command
aaaaabbbbbbb.eastus.cloudapp.azure[.]com	Domain	Used by PipeMagic

References

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://x.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.