INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 06:58 UTC

Microsoft Defender Zero-Days CVE-2026-41091 & CVE-2026-45498 Actively Exploited: SYSTEM Escalation and DoS

CVE VULNERABILITY | CRITICAL | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0202
Type	CVE Vulnerability
CVE ID	CVE-2026-41091, CVE-2026-45498
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Microsoft Defender Malware Protection Engine <=1.1.26030.3008, Antimalware Platform <=4.18.26030.3011; Microsoft System Center Endpoint Protection; System Center 2012/2012 R2 Endpoint Protection; Windows Security Essentials
Published	2026-05-21T03:49:48
Discovery Source	Rss

Executive Summary

Microsoft has patched two actively exploited zero-day vulnerabilities in its Defender security product line, affecting the Malware Protection Engine and Antimalware Platform deployed across Windows enterprise environments. CVE-2026-41091 allows attackers to gain full administrative control (SYSTEM privilege, equivalent to operating system-level access) of affected endpoints; CVE-2026-45498 can disable endpoint protection at scale, leaving systems undetected and undefended. CISA has added both to the Known Exploited Vulnerabilities catalog with a June 3, 2026 remediation deadline for federal agencies, and the broad deployment of Defender across enterprise Windows fleets makes rapid verification of patch delivery a priority for all organizations.

Technical Analysis

Two zero-days in Microsoft's Defender product line were patched and confirmed as actively exploited before disclosure. CVE-2026-41091 (CVSS 9.5) is a privilege escalation vulnerability rooted in CWE-59 (improper link resolution) and CWE-269 (improper privilege management), mapped to MITRE T1068 (Exploitation for Privilege Escalation) and T1574.010 (Services File Permissions Weakness). Successful exploitation yields SYSTEM-level (administrative) access on the affected host. CVE-2026-45498 is a denial-of-service vulnerability (CWE-400: Uncontrolled Resource Consumption) mapped to T1562.001 (Impair Defenses: Disable or Modify

Tools) and T1499 (Endpoint Denial of Service), capable of disabling Defender protection silently at scale. Affected components: Microsoft Defender Malware Protection Engine <=1.1.26030.3008, Antimalware Platform <=4.18.26030.3011, Microsoft System Center Endpoint Protection, System Center 2012/2012 R2 Endpoint Protection, and Windows Security Essentials. Patches are delivered via automatic definition updates; however, active exploitation during the zero-day window means automatic update completion cannot be assumed and must be verified. No threat actor has been attributed. CISA KEV deadline for FCEB agencies: June 3, 2026. Sources: NVD (nvd.nist.gov), CISA KEV catalog (cisa.gov), Microsoft MSRC advisory.

Action Checklist

1. Step 1: Containment. Immediately identify all endpoints running Microsoft Defender Malware Protection Engine <=1.1.26030.3008 or Antimalware Platform <=4.18.26030.3011 via your EDR or endpoint management console (Intune, SCCM, or equivalent). Isolate any endpoints showing anomalous SYSTEM-level process creation or Defender service disruption events until version verification is complete. Reference Microsoft MSRC advisory for [CVE-2026-41091](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41091) and [CVE-2026-45498](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45498).
2. Step 2: Detection. Query endpoint management and SIEM for Defender engine version across the fleet (target: Engine >1.1.26030.3008, Platform >4.18.26030.3011). In Windows Event Log, review Security log for Event ID 4688 (process creation) with SYSTEM-level token assignments originating from Defender service processes (MsMpEng.exe). Review Windows Defender Operational log (Microsoft-Windows-Windows Defender/Operational, Event IDs 1116, 1117, 5007) for service disruptions, configuration changes, or protection state changes. Prerequisite: Ensure that Microsoft-Windows-Windows Defender/Operational log is enabled and forwarded to your SIEM; if not configured, enable Event ID 5001 (Real-time protection disabled) as a high-priority alert. Correlate with MITRE T1562.001 behavioral indicators: unexpected Defender service stops or real-time protection disabled events. Apply NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs) to ensure log coverage is active across the fleet.
3. Step 3: Eradication. Force immediate definition and engine updates on all affected endpoints via Windows Update, Microsoft Update Catalog, or your endpoint management platform. Target versions: Malware Protection Engine >1.1.26030.3008, Antimalware Platform >4.18.26030.3011. For air-gapped or update-restricted environments, deploy updates manually from the [Microsoft Update Catalog](https://www.catalog.update.microsoft.com). Reference Microsoft MSRC advisory for specific update package identifiers. Apply NIST SI-2 (Flaw Remediation) and CIS 7.3 (Perform Automated Operating System Patch Management) as the remediation baseline.
4. Step 4: Recovery. After update deployment, re-query the full endpoint fleet to confirm version compliance. Validate that Defender real-time protection is active and the service is running on all previously affected hosts (Defender Operational Event ID 5001 indicates real-time protection enabled). Re-enable any endpoints that were isolated. Monitor for re-occurrence of SYSTEM-level process anomalies or protection-state change events for 72 hours post-patch. Apply NIST IR-4 (Incident Handling) and AU-6 (Audit Record Review) during the verification window.
5. Step 5: Post-Incident. Document the gap between patch availability and verified deployment across the fleet; this zero-day window represents the core control failure. Review and strengthen your automatic update verification process: assumed delivery is not verified delivery. Assess whether NIST SI-4 (System Monitoring) coverage is sufficient to detect SYSTEM-level privilege changes and defense-evasion activity

(T1562.001) in real time. Evaluate CIS 7.1 (Vulnerability Management Process) and CIS 7.2 (Remediation Process) for SLA gaps on security-tool-specific patches. Consider whether your patch management process treats security tool updates with the same urgency as OS patches.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal, and external IR retainer immediately if any host shows confirmed CVE-2026-41091 SYSTEM-level child process creation from MsMpEng.exe (Event ID 4688 with MsMpEng.exe parent), or if CVE-2026-45498 indicators (Defender service stopped, real-time protection disabled without authorized change) are observed on hosts processing PII, PHI, or PCI-DSS scoped data, as active exploitation of a CISA KEV item with SYSTEM access on those hosts likely triggers breach notification obligations under HIPAA, state privacy statutes, or PCI-DSS Requirement 12.10.
Recovery Notes	Before returning any previously isolated host to production, verify three conditions independently: Defender Engine version exceeds 1.1.26030.3008, Defender Platform version exceeds 4.18.26030.3011, and real-time protection is confirmed active via Event ID 5001 in the Defender Operational log — do not rely solely on the update mechanism confirming success, as CVE-2026-45498 demonstrated the platform can be manipulated to misreport its own state. Maintain elevated monitoring (Sysmon EventID 1 for MsMpEng.exe parent chains, Defender Operational log tailing) for a minimum of 72 hours post-patch on all previously vulnerable hosts, extending to 7 days on any host where SYSTEM escalation indicators were present. Any host where a confirmed MsMpEng.exe child process anomaly was observed should be treated as potentially compromised and subjected to full forensic triage rather than patch-and-return.
Forensic Artifacts	Windows Security Event Log (Security.evtx) — Event ID 4688 entries where ParentProcessName = C:\Program Files\Windows Defender\MsMpEng.exe: the primary forensic signature of CVE-2026-41091 SYSTEM privilege escalation via the Malware Protection Engine, capturing attacker-spawned processes running under the SYSTEM token inherited from the vulnerable Defender process. | Microsoft-Windows-Windows Defender/Operational Event Log — Event IDs 1116 (malware detected), 1117 (malware action taken), 5001 (real-time protection disabled), 5007 (configuration changed): the primary artifact set for CVE-2026-45498 Antimalware Platform DoS exploitation, where unauthorized configuration changes or service disruption events will appear before protection loss becomes visible to users. | Registry hive HKLM\SOFTWARE\Microsoft\Windows Defender\ (full export): CVE-2026-45498 exploitation targeting the Antimalware Platform may modify DisableRealtimeMonitoring, DisableBehaviorMonitoring, or DisableAntiSpyware values; a timestamped export from the exploitation window establishes whether protection was programmatically disabled by attacker code running under SYSTEM. | MsMpEng.exe process memory image (acquired via WinPmem or Magnet RAM Capture before patching or reboot): CVE-2026-41091 exploitation of the Malware Protection Engine may involve in-memory shellcode injection or heap manipulation within the MsMpEng.exe process address space that leaves no on-disk artifact but is recoverable from a live memory capture taken during or immediately after the exploitation window. | Windows System Event Log — Service Control Manager Event IDs 7036 and 7040 for WinDefend and MsMpEng services: records the exact timestamps when Defender services transitioned to stopped or disabled states, providing the forensic timeline anchor for correlating CVE-2026-45498 DoS activity with subsequent attacker actions taken during the unprotected window on affected endpoints.

Per-Action IR Details

Step 1: Containment — Immediately identify all endpoints running Microsoft Defender Malware Protection Engine <=1.1.26030.3008 or Antimalware Platform <=4.18.26030.3011 via your EDR or endpoint management console (Intune, SCCM, or equivalent). Isolate any endpoints showing anomalous SYSTEM-level process creation or Defender service disruption events until version verification is complete. Reference Microsoft MSRC advisory for CVE-2026-41091 and CVE-2026-45498.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-6 (Least Privilege), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without EDR/Intune, run this PowerShell one-liner across the fleet via PSRemoting or a scheduled task to enumerate engine and platform versions: `Get-MpComputerStatus | Select-Object ComputerName, AMEngineVersion, AMProductVersion | Export-Csv C:\IR\defender_versions.csv -Append`. For air-gapped hosts, collect locally and aggregate manually. Flag any host returning AMEngineVersion -le '1.1.26030.3008' or AMProductVersion -le '4.18.26030.3011' for immediate network isolation via host firewall rule: `netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound` — allowlist only management traffic.

Evidence: Before isolating any endpoint, preserve the following: (1) Full memory image using WinPmem or Magnet RAM Capture — CVE-2026-41091 SYSTEM escalation via MsMpEng.exe may leave shellcode or injected threads resident in memory that will not appear on disk. (2) Copy the Windows Security Event Log (`C:\Windows\System32\winevt\Logs\Security.evtx`) and Defender Operational log (`Microsoft-Windows-Windows Defender%4Operational.evtx`) before isolation severs log forwarding. (3) Record the running process tree at time of isolation: `Get-WmiObject Win32_Process | Select ProcessId, ParentProcessId, Name, CommandLine | Export-Csv C:\IR\proctree.csv` — specifically capture any child processes spawned by MsMpEng.exe (PID lineage is critical for CVE-2026-41091 escalation chain reconstruction). (4) Export the current Defender service state: `sc query WinDefend` and `Get-MpPreference | Select-Object DisableRealtimeMonitoring, DisableBehaviorMonitoring`.

Step 2: Detection — Query endpoint management and SIEM for Defender engine version across the fleet (target: Engine >1.1.26030.3008, Platform >4.18.26030.3011). In Windows Event Log, review Security log for Event ID 4688 (process creation) with SYSTEM-level token assignments originating from Defender service processes (MsMpEng.exe). Review Windows Defender Operational log (Microsoft-Windows-Windows Defender/Operational, Event IDs 1116, 1117, 5007) for service disruptions, configuration changes, or protection state changes. Correlate with MITRE T1562.001 behavioral indicators: unexpected Defender service stops or real-time protection disabled events. Apply NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs) to ensure log coverage is active across the fleet.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, deploy Sysmon (SwiftOnSecurity config baseline) and configure EventID 1 (Process Create) to capture MsMpEng.exe as a parent process — any child process spawned by MsMpEng.exe is anomalous and consistent with CVE-2026-41091 exploitation. Use this PowerShell query locally or via PSRemoting to hunt for the CVE-2026-45498 DoS indicator (Defender service stopped or real-time protection disabled): `Get-WinEvent -LogName 'Microsoft-Windows-Windows Defender/Operational' | Where-Object {$_.Id -in @(1116,1117,5007)} | Select TimeCreated, Id, Message | Export-Csv C:\IR\defender_events.csv`. For T1562.001 correlation without EDR, run: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -like '*MsMpEng*'} | Select TimeCreated, Message`.

Evidence: Before concluding the detection phase, preserve: (1) Windows Security Event Log entries for Event ID 4688 filtered on ParentProcessName = MsMpEng.exe — this is the primary forensic indicator for CVE-2026-41091 SYSTEM token abuse, where Defender's privileged process context is weaponized to spawn attacker-controlled child processes.

(2) Defender Operational log Event ID 5007 (configuration change) entries — CVE-2026-45498 exploitation targeting the Antimalware Platform may manifest as unauthorized registry modifications to `HKLM\SOFTWARE\Microsoft\Windows Defender\` disabling real-time protection. Export this registry hive before remediation. (3) Windows System Event Log for Service Control Manager events (Event ID 7036, 7040) showing WinDefend or MsMpEng service state transitions to 'stopped' — these are direct indicators of CVE-2026-45498 DoS exploitation. (4) Prefetch files at `C:\Windows\Prefetch\` for any unusual executables launched in close temporal proximity to MsMpEng.exe anomalies — attacker tooling dropped post-SYSTEM escalation will appear here if prefetch is enabled.

Step 3: Eradication — Force immediate definition and engine updates on all affected endpoints via Windows Update, Microsoft Update Catalog, or your endpoint management platform. Target versions: Malware Protection Engine >1.1.26030.3008, Antimalware Platform >4.18.26030.3011. For air-gapped or update-restricted environments, deploy updates manually from the Microsoft Update Catalog. Reference Microsoft MSRC advisory for the specific update package identifiers. Apply NIST SI-2 (Flaw Remediation) and CIS 7.3 (Perform Automated Operating System Patch Management) as the remediation baseline.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For environments without Intune/SCCM, trigger an immediate Defender engine update from the command line on each affected host (requires admin rights): `cd 'C:\Program Files\Windows Defender' && MpCmdRun.exe -SignatureUpdate`. For air-gapped networks, download the offline package directly from `https://go.microsoft.com/fwlink/?LinkID=121721&arch=x64` (mpam-fe.exe) and deploy via script or USB. After update, verify version remediation with: `Get-MpComputerStatus | Select AMEngineVersion, AMProductVersion` — confirm Engine >1.1.26030.3008 and Platform >4.18.26030.3011 on every host before removing isolation.

Evidence: Before executing updates, preserve the pre-patch state as forensic baseline: (1) Export registry key `HKLM\SOFTWARE\Microsoft\Windows Defender\Signature Updates` — this records the last signature update timestamp and source, establishing whether the engine was deliberately prevented from updating (consistent with CVE-2026-45498 exploitation blocking definition delivery as a persistence mechanism). (2) Copy the current MsMpEng.exe binary (`C:\Program Files\Windows Defender\MsMpEng.exe`) and its associated DLLs to an evidence locker — version metadata and hash comparison against Microsoft's published binary hashes will confirm whether the vulnerable version was in place at time of potential exploitation. (3) On any host where CVE-2026-41091 SYSTEM escalation indicators were observed, perform a full filesystem timeline using `dir /a /s /od C:\ > C:\IR\fstimeline.txt` before patching to identify attacker-dropped files created during the window of SYSTEM access.

Step 4: Recovery — After update deployment, re-query the full endpoint fleet to confirm version compliance. Validate that Defender real-time protection is active and the service is running on all previously affected hosts (Defender Operational Event ID 5001 indicates real-time protection enabled). Re-enable any endpoints that were isolated. Monitor for re-occurrence of SYSTEM-level process anomalies or protection-state change events for 72 hours post-patch. Apply NIST IR-4 (Incident Handling) and AU-6 (Audit Record Review) during the verification window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without centralized monitoring, set a scheduled task on all previously affected hosts to run every 4 hours for 72 hours post-patch, logging Defender state to a network share: `Get-MpComputerStatus | Select ComputerName, AMEngineVersion, AMProductVersion, RealTimeProtectionEnabled, AMServiceEnabled | Export-Csv \\fileserver\IR\recovery_check.csv -Append`. Monitor the share for any host where RealTimeProtectionEnabled returns False or AMServiceEnabled returns False — these are re-exploitation indicators for CVE-2026-45498. Additionally, keep Sysmon EventID 1 logging active for MsMpEng.exe parent process chains throughout the 72-hour window.

Evidence: During the recovery monitoring window, collect the following to confirm clean state and detect re-exploitation: (1) Defender Operational Event ID 5001 (real-time protection enabled) on each previously isolated host — absence of this event post-patch on a host that was updated is a red flag requiring re-isolation. (2) Windows Security Event Log for Event ID 4624 (logon) with Logon Type 3 or 10 on previously isolated endpoints — if an attacker achieved SYSTEM via CVE-2026-41091 before containment, they may have established remote access credentials or implants that survive patching. (3) Scheduled task enumeration on all previously affected hosts: `schtasks /query /fo CSV /v > C:\IR\scheduled_tasks.csv` — post-SYSTEM escalation persistence via scheduled tasks is a high-probability follow-on TTP and must be baselined against known-good state.

Step 5: Post-Incident — Document the gap between patch availability and verified deployment across the fleet — this zero-day window represents the core control failure. Review and strengthen your automatic update verification process: assumed delivery is not verified delivery. Assess whether NIST SI-4 (System Monitoring) coverage is sufficient to detect SYSTEM-level privilege changes and defense-evasion activity (T1562.001) in real time. Evaluate CIS 7.1 (Vulnerability Management Process) and CIS 7.2 (Remediation Process) for SLA gaps on security-tool-specific patches. Consider whether your patch management process treats security tool updates with the same urgency as OS patches.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without a formal vulnerability management platform, establish a lightweight detection baseline for future Defender engine version drift using a weekly scheduled PowerShell script deployed via GPO: `Get-MpComputerStatus | Where-Object {$_.AMEngineVersion -lt 'CURRENT_BASELINE'} | Export-Csv \\fileserver\IR\version_drift.csv`. Update the CURRENT_BASELINE variable each time Microsoft releases a new engine version. Additionally, create a Sigma rule (saved to your detection library) targeting Windows Security Event Log for Event ID 4688 where ParentImage ends in MsMpEng.exe — this will catch any future exploitation of Defender engine vulnerabilities with the same SYSTEM escalation pattern as CVE-2026-41091.

Evidence: For the post-incident report and lessons-learned record, assemble: (1) The full fleet version timeline — first vulnerable version detected, first patch push initiated, last non-compliant host remediated — this quantifies the exposure window for CVE-2026-41091 and CVE-2026-45498. (2) Any Defender Operational Event ID 5007 (configuration change) or 1116/1117 (malware detected/action taken) entries from the exposure window that were not actioned — these represent potential missed exploitation events and must be reviewed against the SYSTEM escalation indicators from Detection. (3) Registry export of `HKLM\SOFTWARE\Microsoft\Windows Defender\` from at least one confirmed-vulnerable host captured pre-patch — provides a forensic reference for any unauthorized configuration modifications consistent with CVE-2026-45498 Antimalware Platform tampering. (4) Process creation audit (Event ID 4688) for MsMpEng.exe parent relationships across the entire exposure window — any findings must be treated as confirmed compromise requiring full host forensic review, not just patching.

Detection Guidance

Primary detection targets: (1) Defender engine and platform version verification, use your endpoint management platform (Intune, SCCM, Group Policy reporting) or EDR to pull current Malware Protection Engine and Antimalware Platform versions fleet-wide; flag any endpoint below Engine 1.1.26030.3008 or Platform 4.18.26030.3011 as unpatched. (2) Privilege escalation indicators, query Windows Security Event Log for Event ID 4688 (new process creation) with ProcessTokenElevationType = TokenElevationTypeFull and ParentProcessName matching MsMpEng.exe or related Defender processes. Correlate with Event ID 4672 (special privileges assigned to new logon) for SYSTEM-level assignments originating from Defender service context. (3) Defense impairment indicators, monitor Microsoft-Windows-Windows Defender/Operational log for

Event IDs 5001 (real-time protection disabled), 5007 (configuration changed), 1116/1117 (malware detected/action taken anomalies). Sudden real-time protection state changes without corresponding admin activity are high-fidelity indicators of CVE-2026-45498 exploitation. Prerequisite: Ensure Microsoft-Windows-Windows Defender/Operational log is enabled and forwarded to your SIEM. (4) Behavioral pattern: T1562.001, unexpected Defender service stops, registry modifications to HKLM\SOFTWARE\Microsoft\Windows Defender\, or scheduled task creation immediately following a Defender service disruption event. Apply NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) to ensure these event sources are captured and reviewed. No confirmed public IOCs (IPs, domains, hashes) are available at this time; attribution remains unknown.

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1574.010** — Services File Permissions Weakness
- **T1562.001** — Disable or Modify Tools
- **T1499** — Endpoint Denial of Service
- **T1203** — Exploitation for Client Execution

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SC-5** — Denial-of-Service Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **IR-5** — Incident Monitoring

CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1574.010	Services File Permissions Weakness	Persistence
T1562.001	Disable or Modify Tools	Defense-Evasion
T1499	Endpoint Denial of Service	Impact
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/microsoft-warns-of-n...	T3
CVE-2026-45498 Detail - NVD - NIST	https://nvd.nist.gov/vuln/detail/CVE-2026-45498	T1
CISA Adds Seven Known Exploited Vulnerabilities to Catalog	https://www.cisa.gov/news-events/alerts/2026/05/20/cisa-adds-seven-...	T1
CVE-2026-41091 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-41091	T3
Microsoft Defender Multiple Vulnerabilities	https://www.hkcert.org/security-bulletin/microsoft-defender-multipl...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-41091, CVE-2026-45498	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-4109...	T1

Generated 2026-05-21 06:58 UTC by TJS Security Command Center