INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 06:49 UTC

Unpatched Windows Defender LPE Zero-Days (RedSun, UnDefend) Under Active Exploitation After PoC Leak, CVE-2026-33825 (BlueHammer) Patched

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0047
Type	CVE Vulnerability
CVE ID	CVE-2026-33825
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0004 (12th percentile)
Affected Products	Microsoft Windows 10, Windows 11, Windows Server 2019 and later, Microsoft Defender
Published	2026-04-17T02:14:52
Discovery Source	Rss

Executive Summary

Three Windows privilege escalation zero-days were publicly disclosed following a proof-of-concept leak; Microsoft patched only one (CVE-2026-33825, BlueHammer) in the April 2026 Patch Tuesday cycle, leaving RedSun and UnDefend unpatched and actively exploited. According to Huntress threat intelligence, a hands-on-keyboard threat actor gained initial access through a compromised SSL VPN account on April 10, 2026, then escalated privileges using one of these vulnerabilities. Any organization running Windows 10, Windows 11, or Windows Server 2019 and later faces immediate risk of full SYSTEM-level compromise on unpatched endpoints, with UnDefend carrying the additional capability to disable Defender antivirus updates.

Technical Analysis

CVE-2026-33825 (BlueHammer) is a local privilege escalation vulnerability in Microsoft Windows and Microsoft Defender, patched in the April 2026 Patch Tuesday cycle. Two additional zero-days, RedSun and UnDefend, remain unpatched as of report date and do not yet have assigned CVE IDs (confidence: medium, pending NVD or CISA confirmation). All three allow escalation to SYSTEM-level privileges on Windows 10, Windows 11,

Windows Server 2019, and later. UnDefend additionally blocks Microsoft Defender antivirus signature updates, degrading endpoint detection capability post-exploitation. CWE classifications: CWE-59 (link following), CWE-269 (improper privilege management), CWE-284 (improper access control). CVSS base score: 9.5 (critical). EPSS: verify score and percentile alignment from NVD; active exploitation is confirmed and supersedes EPSS as the actionable signal. MITRE ATT&CK techniques: T1068 (Exploitation for Privilege Escalation), T1562.001 (Impair Defenses: Disable or Modify Tools), T1543 (Create or Modify System Process), T1059 (Command and Scripting Interpreter), T1203 (Exploitation for Client Execution), T1078 (Valid Accounts). Confirmed intrusion vector includes a compromised SSL VPN account used for post-access lateral movement and privilege escalation. PoC author identified as researcher 'Nightmare-Eclipse'; active exploitation attributed to hands-on-keyboard operator (source: Huntress threat intelligence). Sources: NVD CVE-2026-33825 detail (T1), Microsoft MSRC advisory (T1), Huntress threat report (T2).

Action Checklist

1. Step 1: Containment. Apply the April 2026 Patch Tuesday update for CVE-2026-33825 (BlueHammer) immediately to all Windows 10, Windows 11, and Windows Server 2019+ systems via Microsoft MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825. For RedSun and UnDefend, no vendor patch is available; enforce least-privilege by removing local admin rights from standard user accounts, implement Windows Defender Application Control (WDAC) or AppLocker to restrict binary execution in writable directories, and enforce account lockout policies on interactive logon to constrain the initial escalation path.
2. Step 2: Detection. Review Windows Security Event Log for Event ID 4672 (special privileges assigned to new logon) and Event ID 4688 (process creation with elevated privileges) on endpoints. Hunt for unexpected SYSTEM-level process spawns from non-SYSTEM parent processes. Audit SSL VPN logs for account access anomalies around and after April 10, 2026. Check Defender update status on all endpoints using Microsoft Defender for Endpoint Portal or PowerShell query: Get-MpSignature | Select-Object -Property SignatureVersion, LastUpdated; endpoints failing to receive signature updates may indicate UnDefend activity (T1562.001). Query EDR telemetry for T1068 and T1543 patterns.
3. Step 3: Eradication. For BlueHammer: confirm the April 2026 cumulative update is installed on all in-scope systems using WSUS, SCCM, or equivalent patch management telemetry. For RedSun and UnDefend: no eradication patch exists; isolate any confirmed compromised hosts, re-image if hands-on-keyboard activity is confirmed, and rotate all credentials on affected systems. Revoke and reissue the compromised VPN account credentials identified in the confirmed intrusion vector.
4. Step 4: Recovery. Validate Defender signature currency on all endpoints post-remediation. Confirm SYSTEM-level process anomalies have ceased via EDR. Re-enable and verify Defender real-time protection is active. Monitor VPN authentication logs for re-entry attempts using previously compromised accounts. Run a privileged account audit across affected systems to identify any persistence mechanisms (T1543, T1078).
5. Step 5: Post-Incident. Conduct a review of VPN account lifecycle controls; the confirmed intrusion via a compromised VPN account indicates gaps in credential hygiene or multi-factor authentication enforcement. Evaluate whether LAPS or a PAM solution is deployed on endpoints; while these do not prevent the initial LPE, they constrain the reuse of stolen admin credentials during lateral movement post-exploitation. Submit RedSun and UnDefend identifiers to your threat intelligence platform for tracking; re-evaluate remediation status when CVE IDs and vendor patches are released. Update detection rules to include T1562.001 indicators targeting Defender update blocking.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if hands-on-keyboard activity is confirmed on any host (per Huntress SOC indicators), if the compromised VPN account accessed systems containing PII, PHI, or PCI-scoped data triggering breach notification obligations under applicable regulations, or if RedSun or UnDefend exploitation is detected on hosts where no compensating controls have been applied and no vendor patch is available.
Recovery Notes	Post-containment recovery must validate not only BlueHammer patch installation but specifically that Microsoft Defender real-time protection and signature updates have resumed on all endpoints, as UnDefend's mechanism (T1562.001) may have silently disabled protection before exploitation occurred. Monitor VPN authentication logs and privileged account usage for a minimum of 30 days post-credential rotation, given that Huntress confirmed hands-on-keyboard activity suggesting the threat actor may have established secondary access paths beyond the initial compromised VPN account. Do not return isolated hosts to production until a clean re-image is confirmed or Sysinternals Autoruns and a privileged account audit have cleared them of T1543 and T1078 persistence artifacts specific to this intrusion.
Forensic Artifacts	Windows Security Event Log — Event IDs 4672 (Special Privileges Assigned) and 4688 (Process Creation) filtered on SYSTEM-context spawns from non-SYSTEM parent processes: primary execution trace left by BlueHammer/RedSun/UnDefend LPE exploitation on Windows 10/11/Server 2019+ | Microsoft-Windows-Windows Defender/Operational log — Event IDs 5001 (real-time protection disabled), 5007 (configuration changed), and 5010/5012 (update/scan failure): artifacts specific to UnDefend's T1562.001 Defender tampering mechanism and distinguishable from normal update failures by clustering around the exploitation window | SSL VPN authentication logs for the confirmed compromised account — session timestamps, source IPs, and session duration records from April 10, 2026 onward: establishes lateral movement timeline and scope of network access post-initial-compromise before Huntress SOC detection | Volatile memory dump (WinPmem or equivalent) from any host with confirmed hands-on-keyboard activity — RedSun and UnDefend are unpatched kernel-path LPE exploits whose injected code, shellcode stubs, or token manipulation artifacts exist only in kernel memory and are destroyed on reboot | File system artifacts in C:\Windows\Temp, C:\Users\\AppData\Local\Temp, and C:\ProgramData — staging directories where hands-on-keyboard threat actors (per Huntress SOC confirmed TTPs) drop post-exploitation tools and lateral movement utilities following LPE success

Per-Action IR Details

Step 1: Containment — Apply the April 2026 Patch Tuesday update for CVE-2026-33825 (BlueHammer) immediately to all Windows 10, Windows 11, and Windows Server 2019+ systems via Microsoft MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825. For RedSun and UnDefend, no vendor patch is available; enforce least-privilege on all local accounts and restrict interactive logon rights on high-value systems as interim controls.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch

Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For teams without WSUS/SCCM: run 'wmic qfe list full | findstr KB' on each host to confirm patch installation, or use a PowerShell one-liner: 'Get-HotFix | Where-Object {$_.InstalledOn -gt (Get-Date).AddDays(-30)}'. For least-privilege enforcement on unpatched RedSun/UnDefend systems, use 'net localgroup Administrators' to audit local admin membership and remove non-essential accounts. Deploy Sysmon with the SwiftOnSecurity config to capture process creation events before restricted logon policies are enforced.

Evidence: Before applying the patch, capture: (1) output of 'systeminfo' and 'wmic qfe list' on all in-scope hosts to establish a pre-patch baseline; (2) a snapshot of local Administrators group membership via 'net localgroup Administrators > admins_baseline.txt'; (3) Windows Security Event Log entries for Event ID 4672 (Special Privileges Assigned to New Logon) and Event ID 4673 (Privileged Service Called) in the 72-hour window preceding containment, as BlueHammer/RedSun/UnDefend LPE exploits will leave SYSTEM-level privilege assignment records tied to the exploiting process's PID; (4) current Defender update timestamps from 'Get-MpComputerStatus | Select AntivirusSignatureLastUpdated,RealTimeProtectionEnabled' to detect UnDefend-related tampering before remediation overwrites state.

Step 2: Detection — Review Windows Security Event Log for Event ID 4672 (special privileges assigned to new logon) and Event ID 4688 (process creation with elevated privileges) on endpoints. Hunt for unexpected SYSTEM-level process spawns from non-SYSTEM parent processes. Audit SSL VPN logs for account access anomalies around and after April 10, 2026. Check Defender update status on all endpoints — endpoints failing to receive signature updates may indicate UnDefend activity (T1562.001). Query EDR telemetry for T1068 and T1543 patterns.

NIST Phase: Detection Analysis

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without EDR, deploy Sysmon (Event ID 1 — Process Creation, Event ID 10 — ProcessAccess) and filter for processes where ParentImage is not lsass.exe or services.exe but GrantedAccess includes SYSTEM token. Use this PowerShell to identify Defender tampering: 'Get-WinEvent -LogName "Microsoft-Windows-Windows Defender/Operational" | Where-Object {$_.Id -in @(5001,5004,5007,5010,5012)} | Select TimeCreated,Message'. For VPN log analysis without SIEM, export VPN auth logs to CSV and use 'Import-Csv vpn_logs.csv | Where-Object {$_.Timestamp -ge "2026-04-10" } | Group-Object Username | Sort-Object Count -Descending' to surface high-frequency or off-hours logons. Reference Sigma rule 'win_security_susp_lpe_exploit.yml' for SYSTEM spawn detection.

Evidence: Capture before triage concludes: (1) Windows Security Event Log events 4672 and 4688 filtered on ProcessName spawned under NT AUTHORITY\SYSTEM where ParentProcessName is an unexpected service or user-space process — this is the primary LPE exploitation trace for BlueHammer/RedSun/UnDefend kernel-path escalations; (2) Microsoft-Windows-Windows Defender/Operational log Event IDs 5001 (real-time protection disabled), 5004, 5007 (configuration changed), and 5010/5012 (scan/update failures) as UnDefend specifically targets Defender's update and protection stack (T1562.001); (3) SSL VPN authentication logs for the account confirmed compromised by Huntress SOC, specifically any logon timestamps between April 10–present with source IPs outside known corporate egress ranges; (4) Sysmon Event ID 10 (ProcessAccess) records where a non-privileged process calls OpenProcess on lsass.exe or winlogon.exe, consistent with token impersonation paths used in Windows LPE exploits of this class.

Step 3: Eradication — For BlueHammer: confirm the April 2026 cumulative update is installed on all in-scope systems using WSUS, SCCM, or equivalent patch management telemetry. For RedSun and UnDefend: no eradication patch exists; isolate any confirmed compromised hosts, re-image if hands-on-keyboard activity is confirmed, and rotate all credentials on affected systems. Revoke and reissue the compromised VPN account credentials identified in the confirmed intrusion vector.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without WSUS/SCCM, validate BlueHammer patch deployment using: 'Get-HotFix | Where-Object {$_.HotFixID -eq "KB"}' — replace KB number with the specific cumulative update KB published in the April 2026 MSRC advisory. For hosts confirmed compromised by RedSun or UnDefend where re-imaging is not immediately feasible, use Sysinternals Autoruns (autorunsc.exe -a * -c > autoruns_output.csv) to enumerate all persistence mechanisms before wiping, and run 'net user /domain' plus 'net localgroup Administrators' to identify any accounts added by the threat actor. Immediately disable the compromised VPN account in Active Directory: 'Disable-ADAccount -Identity ' and force a Kerberos ticket purge: 'klist purge' on all authenticated sessions.

Evidence: Before re-imaging or credential rotation, preserve: (1) a full memory dump from any host with confirmed hands-on-keyboard activity (use WinPmem or ProcDump) — RedSun and UnDefend kernel LPE exploits may leave shellcode or injected modules in kernel memory that disappear on reboot; (2) a disk image or at minimum a shadow copy of C:\Windows\Temp, C:\Users\\AppData\Local\Temp, and C:\ProgramData for dropper or tool staging artifacts left by the threat actor post-LPE; (3) Windows Security Event Log Event ID 4720 (account created), 4732 (member added to local group), and 4648 (explicit credential use) from the period of confirmed intrusion — hands-on-keyboard actors routinely create persistence accounts after LPE; (4) VPN session logs for the compromised account showing full session duration, source IP, and bytes transferred to scope potential data access before credential rotation.

Step 4: Recovery — Validate Defender signature currency on all endpoints post-remediation. Confirm SYSTEM-level process anomalies have ceased via EDR. Re-enable and verify Defender real-time protection is active. Monitor VPN authentication logs for re-entry attempts using previously compromised accounts. Run a privileged account audit across affected systems to identify any persistence mechanisms (T1543, T1078).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-2 (Account Management), CIS 8.2 (Collect Audit Logs), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without EDR for post-recovery validation, use: 'Get-MpComputerStatus | Select AntivirusSignatureAge, RealTimeProtectionEnabled, AntivirusEnabled' on all endpoints — flag any host where SignatureAge exceeds 3 days or RealTimeProtectionEnabled is False as potentially still under UnDefend influence. For T1543 persistence hunting without EDR, run Sysinternals Autoruns filtered on non-Microsoft entries: 'autorunsc.exe -m -c > autoruns_clean.csv' and diff against the pre-incident baseline. For T1078 (valid accounts) persistence, query AD for accounts with last password set date during the intrusion window: 'Search-ADAccount -PasswordNeverExpires | Where-Object {$_.PasswordLastSet -ge "2026-04-10"}'.

Evidence: During recovery validation, collect: (1) Microsoft-Windows-Windows Defender/Operational Event ID 1150 and 1151 (signature update success/failure) for all endpoints to confirm UnDefend tampering has been fully reversed; (2) a re-run of Sysmon Event ID 1 process creation logs filtered on SYSTEM-context spawns to confirm LPE activity has ceased — compare against the anomaly baseline captured in Step 2; (3) VPN authentication logs for 30 days post-credential rotation, specifically filtering on the revoked account's username and any accounts that authenticated from the same source IPs identified in the confirmed intrusion; (4) Windows Security Event ID 7045 (new service installed) and 4697 (service installed in the system) to detect T1543.003 (Windows Service) persistence installed by the threat actor during the hands-on-keyboard phase.

Step 5: Post-Incident — Conduct a review of VPN account lifecycle controls; the confirmed intrusion via a compromised VPN account indicates gaps in credential hygiene or MFA enforcement. Evaluate whether LAPS or a PAM solution is deployed on endpoints — these vulnerabilities exploit local privilege paths that PAM controls can constrain. Submit RedSun and UnDefend identifiers to your threat intelligence platform for tracking; re-evaluate remediation status when CVE IDs and vendor patches are released. Update detection

rules to include T1562.001 indicators targeting Defender update blocking.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IA-5 (Authenticator Management), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without a commercial TIP, create a local watchlist for RedSun and UnDefend by adding known IOC patterns to a YARA rule targeting dropper staging paths (C:\Windows\Temp, C:\ProgramData) and known exploit tool names referenced in the Huntress SOC disclosure. Write a Sigma rule targeting Defender tamper Event IDs 5001/5004/5007 and schedule it as a daily PowerShell task: 'Get-WinEvent -LogName "Microsoft-Windows-Windows Defender/Operational" -FilterXPath "*[System[EventID=5001 or EventID=5004 or EventID=5007]]" | Export-Csv defender_tamper_daily.csv'. For LAPS gap assessment without budget, use the free Microsoft LAPS tool (available via Microsoft Download Center) and run 'Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd | Where-Object {$_["ms-Mcs-AdmPwd"] -eq $null}' to identify endpoints without LAPS-managed local admin passwords.

Evidence: For the post-incident review, assemble: (1) the full VPN authentication history for the compromised account for 90 days pre-intrusion to determine if credential compromise predated April 10 and whether initial access was via password spray, phishing, or infostealer — this scopes the breach timeline beyond the Huntress SOC confirmation date; (2) a comparison of Defender signature update history across the fleet to identify any endpoints that stopped receiving updates before April 10, 2026, which may indicate UnDefend was deployed as a precursor to BlueHammer/RedSun exploitation; (3) AD audit logs (Event ID 4738 — user account changed, 4728 — member added to global group) for the 30 days preceding discovery to identify threat actor account manipulation that persisted through eradication; (4) lessons-learned documentation per NIST 800-61r3 §4.1 capturing the gap between VPN account compromise and detection — this metric directly informs MFA enforcement prioritization for CIS 6.4 remediation.

Detection Guidance

Primary detection focus: privilege escalation from standard user to SYSTEM context without a corresponding authorized administrative action. Key Windows Event IDs: 4672 (special privileges assigned), 4688 (process creation, filter for SYSTEM-owned processes spawned by non-SYSTEM parents), 4624/4625 (logon success/failure, cross-reference VPN authentication logs for the April 10+ window). EDR behavioral: look for token impersonation or link-following abuse patterns consistent with CWE-59 and CWE-269, specifically, symlink or junction abuse in writable directories (e.g., %TEMP%, %APPDATA%). For UnDefend (T1562.001): alert on Defender signature update failures or Defender service disruptions not attributable to known maintenance windows; query MDE or equivalent for 'Defender update blocked' events. VPN: audit SSL VPN session logs for accounts that authenticated successfully but show unusual source IPs, geolocations, or session durations post-April 10. Private intelligence (Huntress) has identified indicators of compromise (IOCs) associated with the April 10 intrusion; organizations with Huntress detection should cross-reference those indicators. Public IOCs have not been disclosed; rely on behavioral detection methods outlined above.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available in source data`	Behavioral indicators are the primary detection signal; no hashes, IPs, or domains have been publicly confirmed as associated with active exploitation campaigns as of report date	LOW

Framework Mappings

MITRE-ATTACK

- **T1562.001** — Disable or Modify Tools
- **T1068** — Exploitation for Privilege Escalation
- **T1543** — Create or Modify System Process
- **T1059** — Command and Scripting Interpreter
- **T1203** — Exploitation for Client Execution
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **SC-13** — Cryptographic Protection
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

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

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **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

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(e)(1)** — Transmission Security

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1543	Create or Modify System Process	Persistence
T1059	Command and Scripting Interpreter	Execution
T1203	Exploitation for Client Execution	Execution
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/recently-leaked-wind...	T3
	https://www.bleepingcomputer.com/news/security/recently-leaked-wind...	T3
	https://www.bleepingcomputer.com/news/security/google-fixes-eighth-...	T3
	https://www.bleepingcomputer.com/news/security/cisa-orders-feds-to-...	T3
CVE-2026-33825 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33825	T1

Source	URL	Tier
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825	**T1**

Generated 2026-04-17 06:49 UTC by TJS Security Command Center