INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-28 06:46 UTC

Critical Notepad++ Vulnerabilities Enable Arbitrary Code Execution, Three CVEs Patched

CVE VULNERABILITY | CRITICAL

SCC Item ID	SCC-CVE-2026-0235
Type	CVE Vulnerability
CVE ID	CVE-2025-15556
Severity	CRITICAL
EPSS Score	0.0609 (91th percentile)
Affected Products	Notepad++ (Windows), specific version range unconfirmed from available sources; patch released
Published	58 minutes ago
Discovery Source	Serper

Executive Summary

Notepad++, a widely used Windows text editor installed across development, IT, and administrative workstations, has released patches addressing two confirmed critical vulnerabilities (CVE-2025-15556, CVE-2025-49144). A third vulnerability referenced in news coverage could not be confirmed from available sources. Any organization with Notepad++ on managed endpoints should treat confirmed CVEs as a priority patching event, particularly where the tool is used by users with elevated system access.

Technical Analysis

Two vulnerabilities in Notepad++ for Windows have been confirmed: CVE-2025-15556 and CVE-2025-49144, both rated critical. CVE-2025-15556 is registered in NVD; detailed vulnerability description and affected version data were not accessible from the public NVD record at analysis time. CVE-2025-49144 details are based on SOCPrime blog post; NVD record was not accessed. A third CVE is referenced in news coverage but its identifier could not be confirmed from available sources. MITRE ATT&CK techniques mapped to this advisory: T1203 (Exploitation for Client Execution) and T1068 (Exploitation for Privilege Escalation). CWE classification was not found in available sources (NVD public record and vendor advisory). CVSS base score is pending NVD publication; qualitative rating reflects vendor advisory and exploitation impact assessment. EPSS score for CVE-2025-15556 is 0.061 (6.1% exploitation probability), ranking at the 90th percentile among all disclosed CVEs, indicating elevated active-risk monitoring priority. Specific affected version range is unconfirmed from available sources. Patches have been released. No CISA KEV listing at time of analysis. No confirmed exploitation in the wild or threat actor attribution from available sources.

Action Checklist

1. Step 1: Inventory. List all Windows endpoints where Notepad++ is installed using your asset management system or EDR platform (maps to CIS 1.1). Until patched, block Notepad++ execution via application control on high-value or privileged workstations where possible. Cross-reference software inventory per CIS 2.1.
2. Step 2: Detection. Query endpoint logs and EDR telemetry for Notepad++ process activity spawning child processes (indicative of T1203 client execution abuse). Monitor for privilege escalation patterns from Notepad++ process context (T1068). Review AU-2 (Event Logging) coverage to confirm process creation and privilege-use events are being captured. No confirmed IOCs are available from current sources; behavioral detection is the primary method.
3. Step 3: Eradication. Update Notepad++ to the latest available release from the official Notepad++ project website (verify official domain independently before download). Specific patch version was not confirmed from available sources; verify the installed version against the official release changelog. Apply per CIS 7.4 (Perform Automated Application Patch Management). Remove unauthorized or unmanaged installations per CIS 2.3 (Address Unauthorized Software).
4. Step 4: Recovery. After patching, verify the updated version is deployed across all inventoried endpoints. Confirm no unauthorized processes were spawned from Notepad++ in the window prior to patching using EDR process tree review. Monitor for anomalous privilege use on previously exposed hosts per NIST SI-4 (System Monitoring). Validate audit logging is intact per AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Review application allowlisting policy to confirm third-party tools like Notepad++ are tracked and patched under a defined SLA. Assess whether least-privilege controls (NIST AC-6) limit the blast radius of a successful code execution on affected workstations. Update the software patch management process to include community and open-source tools, which may not appear in commercial patch feeds.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to full IR engagement and legal/compliance notification if any endpoint shows Notepad++ spawning a child process (cmd.exe, powershell.exe, or network-connecting process) during the exposure window, or if Event ID 4672/4673 indicates privilege escalation from Notepad++ context on a host storing PII, PHI, or credentials — either condition indicates likely successful exploitation and may trigger breach notification obligations.
Recovery Notes	After confirming patch deployment across all inventoried endpoints, maintain heightened monitoring on hosts where Notepad++ ran during the exposure window for a minimum of 14 days, focusing on anomalous outbound network connections, new scheduled tasks (Event ID 4698), and new service installations (Event ID 7045) that could indicate post-exploitation persistence. Verify the Notepad++ plugin directory (`C:\Program Files\Notepad++\plugins\`) on all previously exposed hosts contains only vendor-distributed DLLs — compare file hashes against the official Notepad++ GitHub release manifest for the installed version. For any host that cannot be confirmed clean through log review, treat as potentially compromised and escalate to full forensic triage before returning to production use.

Forensic Artifacts	Windows Security Event Log Event ID 4688 (Process Creation) with ParentProcessName = notepad++.exe — captures any code execution chain initiated via CVE-2025-15556 exploitation during the exposure window | Sysmon Event ID 1 process creation and Event ID 3 network connection logs for notepad++.exe — reveals child process spawning and any C2 callback initiated from the Notepad++ process context | Notepad++ plugin directory at C:\Program Files\Notepad++\plugins\ — file hash comparison against official release manifest detects malicious DLL injection or persistence implants dropped post-exploitation | Registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall (DisplayVersion for Notepad++) and HKCU\Software\Notepad++ — documents pre-patch version for exposure confirmation and captures any attacker-modified configuration | Windows Security Event ID 4672 (Special Privileges Assigned) and 4673 (Privileged Service Called) correlated temporally with notepad++.exe execution events — primary forensic indicator of successful CVE-2025-49144 privilege escalation chaining

Per-Action IR Details

Step 1: Containment — Identify all endpoints with Notepad++ installed using your asset inventory (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory). Until patched, consider restricting Notepad++ execution via application control policy on high-value or privileged workstations. Cross-reference software inventory per CIS 2.1.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software)

Compensating: Run the following PowerShell one-liner across all Windows endpoints via PSRemoting or a configuration management tool to enumerate Notepad++ installations: `Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*','HKLM:\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*' | Where-Object { $_.DisplayName -like '*Notepad++*' } | Select-Object DisplayName, DisplayVersion, InstallLocation, PSComputerName`. For application blocking without EDR, use Windows Software Restriction Policy (SRP) or AppLocker to deny execution of notepad++.exe by hash or path on Tier-0/Tier-1 privileged workstations. For standalone systems, use the built-in Windows Defender Application Control (WDAC) in audit mode first to confirm scope before enforcing.

Evidence: Before restricting execution, capture the current installed version from the registry key `HKLM\SOFTWARE\Notepad++\Notepad++` or from `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` (DisplayVersion field) on each host. Record the notepad++.exe file hash (SHA-256) using `Get-FileHash 'C:\Program Files\Notepad++\notepad++.exe'` — this establishes the pre-patch baseline and enables comparison against known-good hashes from the official Notepad++ release. Also snapshot the Notepad++ plugin directory at `C:\Program Files\Notepad++\plugins\` — malicious plugin DLLs are a known persistence vector in editor-based exploits and would survive a process kill without remediation.

Step 2: Detection — Query endpoint logs and EDR telemetry for Notepad++ process activity spawning child processes (indicative of T1203 client execution abuse). Monitor for privilege escalation patterns from Notepad++ process context (T1068). Review AU-2 (Event Logging) coverage to confirm process creation and privilege-use events are being captured. No confirmed IOCs are available from current sources — behavioral detection is the primary method.

NIST Phase: Detection Analysis

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

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

Vulnerability Management Process)

Compensating: Deploy Sysmon with a configuration that captures Event ID 1 (Process Create) and Event ID 10 (ProcessAccess). Write the following Sysmon/Sigma-compatible detection targeting Notepad++ spawning unexpected child processes: filter on ParentImage ending in `notepad++.exe` with child Image matching `cmd.exe`, `powershell.exe`, `wscript.exe`, `mshta.exe`, `rundll32.exe`, or `regsvr32.exe`. For privilege escalation detection (T1068), monitor Sysmon Event ID 8 (CreateRemoteThread) where the source process is `notepad++.exe`. Use Windows Security Event Log Event ID 4688 (Process Creation) with command-line auditing enabled as a fallback where Sysmon is not deployed — filter on `ParentProcessName` containing `notepad++.exe`. A working Sigma rule base can be referenced from the SigmaHQ repository (human validation of current rule availability recommended).

Evidence: Collect Windows Security Event Log Event ID 4688 records from the 30 days prior to detection, filtering specifically on processes with `notepad++.exe` as the parent — these records will reveal any code execution chain triggered via CVE-2025-15556. Capture Sysmon Event ID 11 (File Create) and Event ID 13 (Registry Value Set) with source process `notepad++.exe` to identify any files dropped or registry keys modified during exploitation. For CVE-2025-49144 (privilege escalation component), look for Windows Security Event ID 4672 (Special Privileges Assigned to New Logon) and Event ID 4673 (Privileged Service Called) in close temporal proximity to notepad++.exe execution events — this sequence would indicate a successful privilege escalation from user context.

Step 3: Eradication — Update Notepad++ to the latest available release via the official Notepad++ site (notepad-plus-plus.org). Specific patch version was not confirmed from available sources; verify the installed version against the official release changelog. Apply per CIS 7.4 (Perform Automated Application Patch Management). Remove unauthorized or unmanaged installations per CIS 2.3 (Address Unauthorized Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST CM-8 (System Component Inventory), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: For teams without a software deployment tool, use winget to deploy the update at scale: `winget upgrade --id Notepad++.Notepad++ --silent --accept-package-agreements` — run this via PSRemoting across all inventoried endpoints. For portable/unregistered Notepad++ installations (common in developer environments), the registry-based inventory query from Step 1 will miss these — additionally search for `notepad++.exe` by running `Get-ChildItem -Path C:\ -Recurse -Filter 'notepad++.exe' -ErrorAction SilentlyContinue` on suspect hosts. Verify post-update file hash against the SHA-256 hash published in the official Notepad++ GitHub release notes for the patched version (human verification of the specific hash from notepad-plus-plus.org/downloads recommended before deployment).

Evidence: Before executing the update, preserve a forensic image or at minimum a file hash inventory of the Notepad++ installation directory (`C:\Program Files\Notepad++\` and any portable locations) and the plugin subdirectory. Capture the Notepad++ configuration file at `%APPDATA%\Notepad++\config.xml` — if an attacker installed a malicious plugin or modified configuration as part of post-exploitation, this file may reference persistence artifacts. Document the exact pre-patch version string from the registry DisplayVersion field on each endpoint to establish the remediation audit trail required for compliance reporting.

Step 4: Recovery — After patching, verify the updated version is deployed across all inventoried endpoints. Confirm no unauthorized processes were spawned from Notepad++ in the window prior to patching using EDR process tree review. Monitor for anomalous privilege use on previously exposed hosts per NIST SI-4 (System Monitoring). Validate audit logging is intact per AU-6 (Audit Record Review, Analysis, and Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-4 (Incident Handling), NIST CA-7 (Continuous Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.2 (Establish and Maintain

a Remediation Process)

Compensating: Use the following PowerShell command to confirm the patched version is deployed on each host via PSRemoting: `Invoke-Command -ComputerName -ScriptBlock { (Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*' | Where-Object { $_.DisplayName -like '*Notepad++*' }).DisplayVersion }`. For process tree review without EDR, query archived Sysmon Event ID 1 logs filtered to the exposure window (date range from when Notepad++ was last known unpatched to patch deployment date) for any child processes of `notepad++.exe`. For anomalous privilege monitoring on previously exposed hosts, enable enhanced auditing for Event ID 4672 and 4673 and review daily for 14 days post-patch.

Evidence: Pull the full process creation log (Sysmon Event ID 1 or Windows Security Event ID 4688) for the exposure window — defined as the period from public disclosure of CVE-2025-15556 (date to be confirmed from NVD publication) through confirmed patch deployment on each host. For any host where Notepad++ spawned a child process during the exposure window, collect the full Sysmon process tree, associated network connection events (Sysmon Event ID 3), and any file creation events (Sysmon Event ID 11) to determine whether exploitation resulted in payload delivery or lateral movement. Verify Windows audit log continuity (no gaps in Event ID sequence) on previously exposed hosts — log clearing via Event ID 1102 (Security Audit Log Cleared) during the exposure window would indicate active attacker presence.

Step 5: Post-Incident — Review application allowlisting policy to confirm third-party tools like Notepad++ are tracked and patched under a defined SLA. Assess whether least-privilege controls (NIST AC-6) limit the blast radius of a successful code execution on affected workstations. Update the software patch management process to include community/open-source tools, which may not appear in commercial patch feeds.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST PM-6 (Measures of Performance), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: For teams without a commercial vulnerability management platform, subscribe to the Notepad++ GitHub releases RSS feed (github.com/notepad-plus-plus/notepad-plus-plus/releases) and the NVD CVE feed filtered to vendor 'notepad-plus-plus' as a manual patch intelligence source. Use osquery to build a persistent inventory query for Notepad++ versioning: `SELECT name, version, install_location FROM programs WHERE name LIKE '%Notepad++%';` — schedule this as a weekly scheduled query to detect version drift after patching. For least-privilege assessment, use the built-in `whoami /priv` command on workstations where Notepad++ is routinely used by admins to confirm SeDebugPrivilege and SeTakeOwnershipPrivilege are not available in standard user context — these would materially increase blast radius if CVE-2025-49144 privilege escalation were successfully chained.

Evidence: Document the time-to-patch metric from public CVE disclosure to confirmed deployment across all endpoints — this becomes the baseline SLA measurement for open-source tool patching going forward. Retain the pre- and post-patch version inventory exports (from the PowerShell registry queries in Steps 1 and 4) as the audit record demonstrating remediation scope and completeness. If any host showed anomalous Notepad++ child process activity during the exposure window, retain those Sysmon logs, Windows Security logs, and any captured memory artifacts for a minimum of 12 months in accordance with your incident record retention policy (NIST AU-11 — Audit Record Retention).

Detection Guidance

No confirmed IOCs (hashes, domains, IPs) are available from current sources. Detection should focus on behavioral indicators. Using EDR or SIEM, query for: Notepad++ process (notepad++.exe) spawning child processes such as cmd.exe, powershell.exe, wscript.exe, or mshta.exe; Notepad++ process context triggering privilege escalation events (Windows Event ID 4672, Special Privileges Assigned to New Logon, Event ID 4688, Process Creation with elevated integrity level); and unexpected DLL loads from Notepad++ process space.

Align log collection coverage with NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation), and CIS 8.2 (Collect Audit Logs). MITRE ATT&CK T1203 and T1068 detection rules in your SIEM/EDR platform should be reviewed and tuned for this process context. D3FEND countermeasure D3-SFA (System File Analysis) is relevant for monitoring unexpected modification of files associated with Notepad++ installation. Note: the EPSS score for CVE-2025-15556 is 0.061 (6.1% exploitation probability), ranking at the 90th percentile among all disclosed CVEs. This positions it in the high-probability category relative to the broader CVE population, indicating elevated active-risk monitoring priority.

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

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

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
	https://cybersecuritynews.com/critical-notepad-vulnerabilities/	T3
CVE-2025-49144 Vulnerability: Critical Privilege Escalation Flaw in ...	https://socprime.com/blog/cve-2025-49144-notepad-vulnerability/	T3
Critical Notepad++ Vulnerability Lets Attackers Execute Malicious ...	https://www.reddit.com/r/pwnhub/comments/1ntc1yp/critical_notepad_v...	T3
CVE-2025-15556 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-15556	T1
Notepad++ Code Execution Vulnerability Exploited in - LinkedIn	https://www.linkedin.com/posts/cybersecurity-news_cybersecuritynews...	T3

Generated 2026-05-28 06:46 UTC by TJS Security Command Center