UPDATE: Notepad++ Update Infrastructure Hijacked via Hosting Provider Compromise

TL;DR

Notepad++ confirmed its update infrastructure was hijacked after attackers compromised a shared hosting provider.

Between June and December 2025, update traffic for selected users was redirected to malicious servers.

Notepad++ source code was not compromised. Users should manually update to the latest version immediately.

UPDATE 2/19/2026

Notepad++ released version 8.9.2 with additional security protections tied to the recent update infrastructure compromise. The update now checks both the signed installer and the signed XML file from the update server, adding another layer of verification to prevent tampering. The update also hardens the WinGUp auto-updater component by removing DLL side-loading risk and tightening plugin execution controls.

Additionally, CVE-2026-25926 (CVSS 7.3) was patched. This Unsafe Search Path vulnerability could allow arbitrary code execution if an attacker can control the working directory when Windows Explorer is launched.

Recommendations

- Update all Notepad++ installations to version 8.9.2 using the official installer.
- Avoid relying on older automatic update workflows.
- Monitor developer systems for unusual explorer.exe execution paths or unsigned plugin activity.
- Continue reviewing systems updated during the June through December 2025 window.

UPDATE 2/4/2026

New third-party analysis shows the Notepad++ update compromise was not limited to a single malicious updater. Activity began as early as June 2025, with confirmed malicious update delivery taking place between July and October 2025. While no new payloads were observed after November 2025, attackers continued rotating infrastructure and update filenames through late October.

Researchers identified at least three execution chains. Two were used to deliver Cobalt Strike via shellcode loaders launched by the legitimate Notepad++ updater. A later chain relied on DLL sideloading to deploy the Chrysalis backdoor, tooling that has been linked in prior reporting to the Chinese state-sponsored threat actor Lotus Blossom (also tracked as Billbug or Thrip). Several stages abused legitimate software components to execute payloads, a pattern consistent with attempts to blend into developer environments.

The activity impacts individual developers and a small number of organizations across government, finance, and IT services. CrowdStrike has referenced the incident at a high level in its threat reporting but has not released any Notepad++-specific indicators of compromise. Rapid7 and Kaspersky GReAT have published the IoCs below. Aspire will continue to monitor this activity and provide updates as new information becomes available.

IoCs

Malicious Update Delivery URLs

- http://45[.]76[.]155[.]202/update/update.exe
- http://45[.]32[.]144[.]255/update/update.exe
- http://95[.]179[.]213[.]0/update/update.exe
- http://95[.]179[.]213[.]0/update/install.exe
- http://95[.]179[.]213[.]0/update/AutoUpdater.exe

System Information Exfiltration

- http://45[.]76[.]155[.]202/list
- https://self-dns[.]it[.]com/list
- temp[.]sh

Payload Loader URLs

- https://45.77.31[.]210/users/admin
- https://cdncheck[.]it.com/users/admin
- https://safe-dns[.]it.com/help/Get-Start

Cobalt Strike Command-and-Control

- https://45[.]77[.]31[.]210/api/update/v1
- https://45[.]77[.]31[.]210/api/FileUpload/submit
- https://cdncheck[.]it.com/api/update/v1
- https://cdncheck[.]it.com/api/Metadata/submit
- https://cdncheck[.]it.com/api/getInfo/v1
- https://safe-dns[.]it.com/resolve
- https://safe-dns[.]it.com/dns-query

Chrysalis / Related Infrastructure (Rapid7)

- https://api[.]skycloudcenter[.]com/a/chat/s/70521ddf-a2ef-4adf-9cf0-6d8e24aaa821
- https://api[.]wiresguard[.]com/update/v1
- https://api[.]wiresguard[.]com/api/FileUpload/submit
- https://api[.]wiresguard[.]com/users/system
- https://api[.]wiresguard[.]com/api/getInfo/v1

Additional Beacon Infrastructure (Rapid7 – multiscanner)

- http://59[.]110[.]7[.]32:8880/uffhxpSy
- http://59[.]110[.]7[.]32:8880/api/getBasicInfo/v1
- http://59[.]110[.]7[.]32:8880/api/Metadata/submit
- http://124[.]222[.]137[.]114:9999/3yZR31VK
- http://124[.]222[.]137[.]114:9999/api/updateStatus/v1
- http://124[.]222[.]137[.]114:9999/api/Info/submit

Malicious File Hashes (SHA1)

- 8e6e505438c21f3d281e1cc257abdbf7223b7f5a
- 90e677d7ff5844407b9c073e3b7e896e078e11cd
- 573549869e84544e3ef253bdba79851dcde4963a
- 13179c8f19fbf3d8473c49983a199e6cb4f318f0
- 4c9aac447bf732acc97992290aa7a187b967ee2c
- 821c0cafb2aab0f063ef7e313f64313fc81d46cd

Auxiliary / loader files

- 06a6a5a39193075734a32e0235bde0e979c27228 (load)
- 9c3ba38890ed984a25abb6a094b5dbf052f22fa7 (load)
- ca4b6fe0c69472cd3d63b212eb805b7f65710d33 (alien.ini)
- 0d0f315fd8cf408a483f8e2dd1e69422629ed9fd (alien.ini)
- 2a476cfb85fbf012fdbe63a37642c11afa5cf020 (alien.ini)

Rapid7-reported payload hashes

- d7ffd7b588880cf61b603346a3557e7cce648c93
- 94dffa9de5b665dc51bc36e2693b8a3a0a4cc6b8
- 21a942273c14e4b9d3faa58e4de1fd4d5014a1ed
- 7e0790226ea461bcc9ecd4be3c315ace41e1c122
- f7910d943a013eede24ac89d6388c1b98f8b3717

Observed Malicious File Paths

- %appdata%\ProShow\load
- %appdata%\Adobe\Scripts\alien.ini
- %appdata%\Bluetooth\BluetoothService

Overview

There is an infrastructure-level compromise affecting the update delivery mechanism in Notepad++. The security incident stems from a breach at the shared hosting provider level, **not from a vulnerability in Notepad++ code**. Attackers gained access to the hosting environment supporting the Notepad++ update endpoint and intercepted update traffic intended for legitimate users.

The hosting provider confirmed the shared server was compromised until September 2, 2025. Although direct server access ended on that date, attackers retained credentials to internal services tied to the environment. This access allowed continued redirection of update traffic until December 2, 2025.

Affected Products

- Notepad++ installations using automatic update functionality during the compromise window, particularly older versions lacking strong update verification controls.

Logs show the attackers specifically targeted the notepad-plus-plus.org domain and its update endpoint. No other customers hosted on the same infrastructure were affected. Attempts to re-exploit the environment after remediation were observed but did not succeed.

Independent security researchers assessed the activity as highly targeted. Based on the scope, the activity is believed to be associated with a Chinese state-sponsored threat actor. The overall compromise window is assessed to have spanned from June through December 2, 2025.

Aspire Protects

- Manually update Notepad++ to the latest available version using the official installer. Do not rely on older automatic update workflows.
- Review systems updated between June and December 2025 for unexpected installers, binaries, or file hashes tied to Notepad++ updates.

- Restrict outbound update traffic where possible and allow updates only from known, trusted domains.
- Monitor developer endpoints for abnormal network redirection, unsigned executables, or execution of installers from non-standard paths.
- Treat developer tools as trusted software within security monitoring and asset inventories.

TTPs to Watch

Initial Access

- Supply Chain Compromise [T1195] – The attacker may have compromised hosting infrastructure supporting the Notepad++ update service, allowing interception and redirection of trusted update traffic.

Execution

- User Execution [T1204] – Users may have executed malicious installers delivered through redirected update requests.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations using Notepad++ in development, engineering, or IT workflows are at risk, particularly where automatic updates were enabled during the compromise window.

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Notepad++ Hijacked by State-Sponsored Hackers | Notepad++
Download Notepad++ v8.9.1 (stable: auto-update triggered) | Notepad++