Smarttech
YOUR 24/7 SECURITY PARTNER

Notepad++ Official Update Mechanism Supply-Chain Compromise

Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	3rd February 2026
Issue Date	3rd February 2026

Informative Cyber Alerts are reports created by Smarttech247 designed to inform customers about medium and low severity vulnerabilities, IOCs from certain attacks/breaches, and other information that could help companies be aware and protect against any attack.
The content of this report should be regarded as simply informative as it usually addresses products that have an auto-update option available for patches. It will be the customer's decision if it is necessary to follow any recommendation or disregard them as they are not currently applicable in the environment.

Overview

A major supply-chain compromise affecting Notepad++'s official update infrastructure was disclosed by the project's maintainers. Between June and December 2025, attackers hijacked the update mechanism by compromising the shared hosting infrastructure used to deliver updates, enabling them to redirect specific users' update requests to attacker-controlled servers that delivered malicious installers.

Technical Summary

The attack focused on the WinGUp (Windows General Upgrader) tool, which is the executable responsible for checking and downloading updates for Notepad++.
Between June and December 2025, attackers compromised the back-end server hosting notepad-plus-plus.org. They did not replace the legitimate installer for everyone. Instead, they implemented a selective redirection script. When a user's client sent an update request, the server checked the originating IP address.

If the IP belonged to a specific list (telecoms, government agencies, or financial sectors in Southeast Asia and Europe), the server redirected the request to a malicious server.

Standard home users received the legitimate, clean update, which allowed the operation to remain undetected by the general public for over six months.

Once the targeted user clicked "Yes" to the update prompt, the hijacked WinGUp downloaded a poisoned package. The attack used a sophisticated DLL Side-Loading technique to bypass EDR (Endpoint Detection and Response) systems:

The package dropped a legitimate, digitally signed binary (often a component of Bitdefender or another trusted security suite) into a temporary directory.
It dropped a malicious DLL named log.dll (or similar) into the same folder.
When the legitimate binary ran, it automatically loaded the malicious log.dll instead of the system version. Because the primary process was "trusted" and signed, many security tools ignored the malicious activity happening in the background.
This loaded the Chrysalis backdoor into memory.

Chrysalis was designed for long-term presence. It established itself in the user's environment using the following methods:
It created a hidden folder at %AppData%\Bluetooth to store its configuration and staging files.
It often registered itself as a service named BluetoothService or UpdateCheck to blend in with standard Windows background tasks.
The malware communicated over HTTPS to api.skycloudcenter[.]com, mimicking standard cloud API traffic to evade network firewalls.

The Chrysalis backdoor provided the Billbug (Lotus Blossom) actors with:

-Remote execution of PowerShell and CMD commands.

- Scraping memory for browser passwords and SSH/Git keys.

- Staging files in the hidden Bluetooth folder before uploading them to the C2 server.

The malware included a "burn" command to wipe all traces of its existence if it detected it was being analyzed or if the mission was complete.

Recommendations

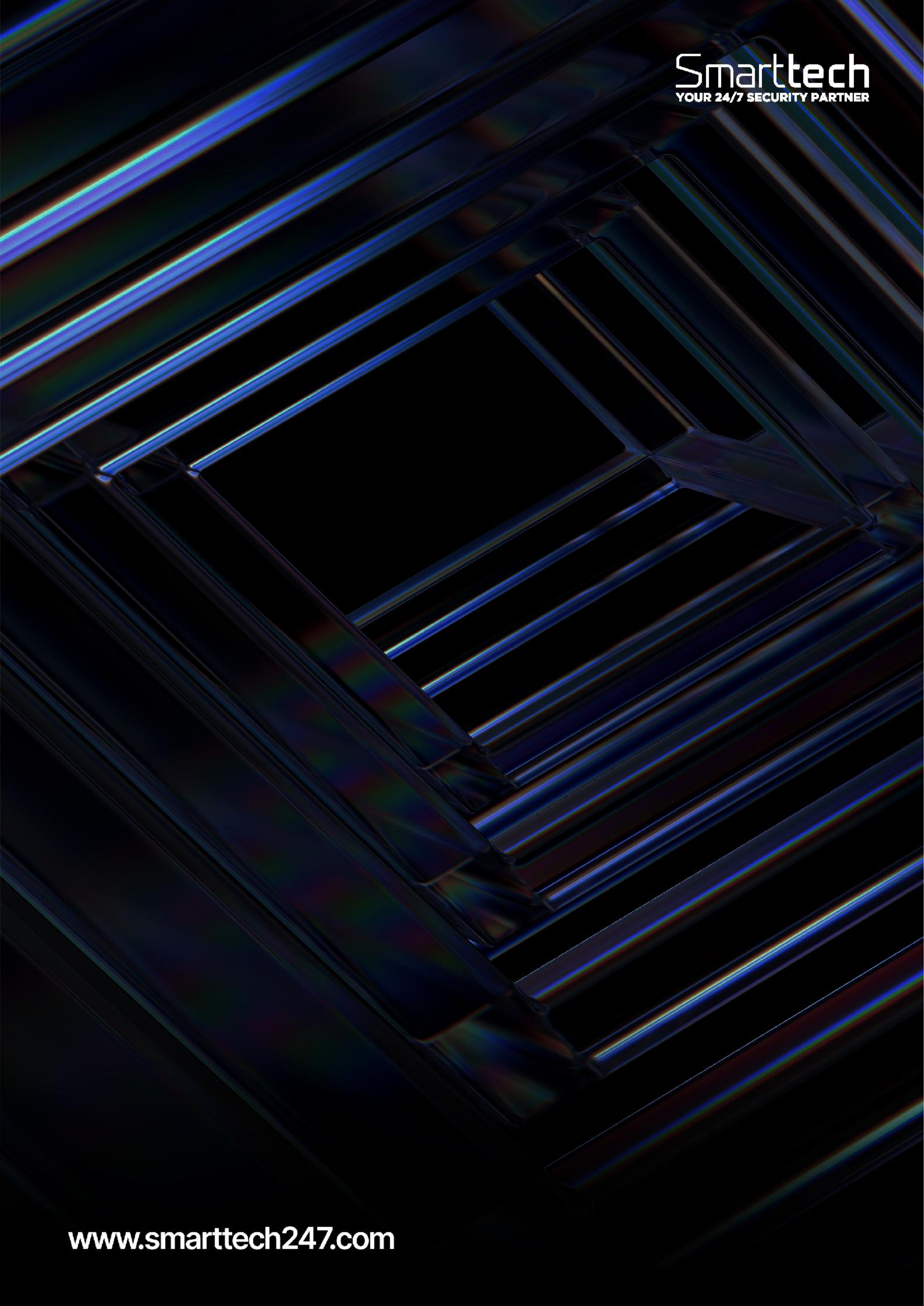
Smarttech247 team recommends the following actions to be taken:

- Verify Installed Version
- Ensure that the installed Notepad++.exe is digitally signed by "Notepad++" and that the signature is valid. If the signature is missing or invalid, treat the system as compromised. (Ref: MITRE ATT&CK M1051)
- If a malicious version is found, follow the standard incident response procedure: isolate the host, wipe the machine, and rotate any credentials stored on that device.
- Ensure all corporate domains and critical third-party tools are protected by Multi-Factor Authentication (MFA) and Registrar Locks at the DNS provider level.
- Maintain a list of "Authorized Software" and ensure users only download tools from verified, non-hijacked sources.

References

https://notepad-plus-plus.org/news/hijacked-incident-info-update/

https://thehackernews.com/2026/02/notepad-official-update-mechanism.html



Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com