EnCyb

Severity: High

Advisory Type: Vulnerability

Notepad++ Supply Chain Breach by CLotus Blossom

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

The threat actor CLotus Blossom has been linked to a supply-chain compromise involving the official hosting infrastructure of Notepad++. Attackers gained unauthorized access to distribution resources and leveraged the trusted platform to host or deliver maliciously modified components, exposing users to potential backdoor installation. By abusing the trust associated with a widely used open-source application, the attackers increased the likelihood of successful compromise while bypassing conventional security warnings. This incident highlights the continued targeting of software supply chains as a high-impact attack vector.

- Active Region: Global
- Affected Sector: Software Development, Enterprises, General Users
- Affected Product: Notepad++ (Official Distribution Infrastructure)
- Severity: High
- Published Date: February 16, 2026

TECHNICAL DETAILS

- **Initial Compromise:** Threat actors compromised the Notepad++ update infrastructure rather than the application source code itself. This represents a software supply-chain attack, where trust in a legitimate vendor distribution channel is abused instead of exploiting a software vulnerability.
- **Malicious Payload Distribution:** Compromised infrastructure was used to serve trojanized installers or components.
- **Execution and Installation:** Malicious code executed during normal software installation or update processes. No additional user interaction beyond installation was required.
- **Post-Installation Capabilities:** C2 and Ability to download and execute additional payloads, enabling modular expansion of the compromise. Persistence mechanisms ensured the malware survived system reboots and software updates. Supported data exfiltration, reconnaissance, and lateral movement, depending on the targeted environment.

IMPACT

- Compromise of systems installing affected Notepad++ components
- Unauthorized remote access and persistent backdoor installation
- Exposure of developer environments and sensitive source code
- Increased risk of follow-on attacks, including espionage and ransomware

RECOMMENDATIONS

- Verify Notepad++ downloads using official checksums and digital signatures
- Reinstall Notepad++ from confirmed clean sources if compromise is suspected
- Restrict outbound network access for developer tools where feasible
- Apply application allow-listing to prevent unauthorized code execution

REFERENCE

- https://gbhackers.com/notepad-breached/
- https://unit42.paloaltonetworks.com/notepad-infrastructure-compromise/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com