مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Supply-Chain Exposure in Notepad++ Update Infrastructure

Tracking #:432318123

Date:12-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Notepad++ users are exposed to a supply-chain style attack where adversaries manipulated the updater's network traffic to deliver malware.

TECHNICAL DETAILS:

Notepad++ users are exposed to a supply-chain style attack where adversaries manipulated the updater's network traffic to deliver malware. Version 8.8.9 introduces robust mitigations and requires manual installation. The WinGUp updater retrieves update URLs from a remote PHP endpoint, downloads installers into the TEMP directory, and executes them. Attackers exploited redirectable traffic and weak signature validation to replace installers. Since v8.8.7, GlobalSign certificates have been used, but strict validation only exists from v8.8.9 onward. Multiple targeted organizations were confirmed affected.

Vulnerability Information

- **Issue Type:** Insecure update delivery
- **Root Cause:** Manipulable XML-sourced download path
- **Abused Files:** %TEMP%\update.exe, %TEMP%\AutoUpdater.exe
- **Detection Indicators:** gup.exe connecting to unknown URLs
- **Severity:** High

Root Cause Factors

1. **Redirectable Network Traffic:**

Attackers intercepted and redirected traffic to malicious infrastructure.

2. **Previous Use of a Self-Signed Certificate (≤ v8.8.7):**
    - A self-signed certificate included openly in the GitHub source code enabled attackers to craft binaries that appeared superficially legitimate.
    - Victims would receive "Unknown Publisher" warnings—which many users ignore.
3. **Insufficient Signature Validation:**
   Earlier versions did not enforce strict signature checks on downloaded installers.

Impacted Versions

- **Affected:** Notepad++ versions **up to v8.8.7** and **v8.8.8** (still vulnerable due to incomplete hardening).
- **Patched: Notepad++ v8.8.9**, which enforces:
    - Mandatory use of trusted download sources (GitHub only).
    - Signature and certificate validation on downloaded installers.
    - Automatic update abortion on validation failure.

RECOMMENDATIONS:

1. **Manually Update Notepad++ to v8.8.9 Immediately**
    - Download only from the official site or GitHub link referenced on that site.
    - Validate the digital signature (GlobalSign certificate).
2. **Verify Update Integrity**
    - Ensure the installer is signed by **Notepad++ (GlobalSign certificate)**.
    - Do not proceed if the publisher appears as "Unknown Publisher".

3. **Perform IOC-Based Threat Hunting**
   - Check network logs for suspicious outbound connections from gup.exe.
   - Inspect for unexpected processes spawned by gup.exe.
   - Review %TEMP% folder for:
     - update.exe
     - AutoUpdater.exe
   - If found, treat systems as potentially compromised.
4. **Conduct Endpoint Malware Scanning**
   - Run full scans using reputable EDR/AV solutions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://notepad-plus-plus.org/news/v889-released/