مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

DLL Hijacking Vulnerability in Notepad++

Tracking #:432317757

Date:29-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a DLL hijacking vulnerability (CVE-2025-56383) was disclosed in Notepad that can enable the attackers to load the malicious DLL and execute arbitrary code in the context of the running user.

TECHNICAL DETAILS:

A DLL hijacking vulnerability (CVE-2025-56383) was disclosed in Notepad++ v8.8.3. An attacker who can place a malicious DLL into the Notepad++ installation or execution path (for example, by writing to the Plugins directory or via a trojanized installer) can cause Notepad++ to load the malicious DLL and execute arbitrary code in the context of the running user. A working proof-of-concept (PoC) demonstrating replacement of NppExport.dll and forwarding to the original DLL while executing malicious code is publicly available.

Vulnerability Details

- CVE: CVE-2025-56383
- Severity: Medium (CVSS ~6.5)
- Affected Software: Notepad++ v8.8.3 (confirmed)
- **Impacts:**
  - Arbitrary code execution when Notepad++ is launched and the forged DLL is loaded. This can be used for persistence, privilege escalation (if Notepad++ is run with elevated rights), lateral movement, or to drop additional malware.
  - Attack scope: Users with Notepad++ v8.8.3 installations are affected. The vulnerability requires the ability to place or replace DLL files in locations that Notepad++ will search at runtime (local access, installer tampering, supply chain or insider threats).

RECOMMENDATIONS:

- Apply file-permission restrictions immediately; validate existing Notepad++ installs and scan for unexpected DLLs.
- Avoid running Notepad++ installers downloaded from untrusted sources.

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.

REFERNCES:

- https://github.com/zer0t0/CVE-2025-56383-Proof-of-Concept
- https://github.com/notepad-plus-plus/notepad-plus-plus