A DLL hijacking bug targets Notepad++. Risk of arbitrary code execution. -

Data: 2025-09-29 10:14:00

Autor: Inteligência Against Invaders

Redazione RHC**:29 September 2025 09:14**

A critical DLL hijacking vulnerability has been identified in Notepad++ version 8.8.3 by security researchers, with the flaw assigned CVE-2025-56383.

The vulnerability specifically targets **the Notepad++ plugin system, specifically the NppExport.dll file** located in the Notepad++pluginsNppExport directory.

This flaw allows attackers to **execute arbitrary code by replacing legitimate Dynamic Link Library (DLL) files** within the application's plugin directory with malicious versions that retain the same export functions.

Attackers can exploit this weakness *by creating a malicious DLL file with identical export functions that forward calls to the original DLL while simultaneously executing malicious code.*

When users launch Notepad++, the application automatically loads these plugin DLLs, creating the opportunity for malicious code execution.

The attack method **involves replacing the original DLL file with a counterfeit version** that appears legitimate but contains embedded malicious functionality.

Successful exploitation of the vulnerability requires attackers *to have access to the local file system and be able to modify files within the Notepad++ installation directory.*

While this limits the scope of the attack to scenarios where attackers already have some level of access to the system, *it can serve as an effective privilege escalation or persistence mechanism.*

The vulnerability was assigned a **CVSS 3.1 score of 7.8 (High),** indicating *significant security implications.*

The attack vector is classified as local with low complexity and requires low privileges and user interaction to succeed.

Security researcher zer0t0 has posted a proof-of-concept on GitHub, showing how the vulnerability can be exploited using the NppExport.dll plugin.

The demonstration involves replacing the original DLL with a malicious version called original-NppExport.dll, while keeping the rogue version of NppExport.dll in its place.

While no official patch has been released yet, **users should exercise caution when downloading Notepad++ from unofficial sources or allowing untrusted software to modify their system.**

Organizations should monitor their Notepad++ installations for unauthorized changes to plugin DLL files.

Since Notepad++ is still widely used in a variety of contexts, fixing this vulnerability is critical for both developers and users.

The vulnerability affects not only version 8.8.3, but potentially also other versions of Notepad++ that use similar plugin loading mechanisms.

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli