Nitro PDF Pro Empty XFA Denial of Service Vulnerability

← Back to Advisories

CVE NUMBER

CVE-2025-66769

VENDOR

Nitro

CREDIT

Abu

Description

A denial-of-service vulnerability exists in Nitro PDF Pro 14.41.1.4. When a specially crafted PDF file containing an empty /XFA [] array within the /AcroForm is opened, the application crashes immediately. Despite the absence of a valid XFA node tree in the file, Nitro PDF Pro continues to execute its XFA processing routine, ultimately leading to a NULL pointer dereference. As a result, simply opening a malicious PDF file can cause the application to terminate abruptly.

Details

The issue arises during the processing of a PDF document in which an `/XFA []` entry is declared within `/AcroForm`, but no actual XFA content is present.

For example, a PDF containing the following structure can trigger the vulnerability:

```
pdf
4 0 obj
<<
/Fields [5 0 R]
/XFA []
>>
endobj
```

When opening such a document, Nitro PDF Pro initializes internal objects for XFA processing and attempts to locate root nodes such as `xdp:xdp` and `template`. However, because the XFA structure is empty, the first lookup returns `0 (NULL)`, and this NULL pointer is subsequently passed to the next lookup operation without validation.

The vulnerable flow can be simplified as follows:

```
v14 = sub_1E8E60(a1 + 0x158, L"xdp:xdp");
v15 = sub_1E8E60(v14,        L"template");
```

The node lookup function fails to validate whether the provided object pointer is NULL before accessing its internal members:

```
__int64 sub_1E8E60(__int64 a1, const wchar_t *a2)
{
    if (!a2)
        return 0;

    a1_0x40 = *(_QWORD *)(a1 + 0x40);
    ...
}
```

As a result, when `a1 == 0`, the expression `*(QWORD *)(a1 + 0x40)` dereferences a NULL pointer, leading to an access violation. Consequently, Nitro PDF Pro terminates immediately upon opening the malicious document.

Timeline

2025-11-19 - Vulnerability reported to Vendor

2026-01-09 - Vendor Patch Release

2026-04-06 - Public Release