

Forum:[Hack Forums](#)

Thread: [CRITICAL Apache Tika XXE CVE-2025-66516 \(CVSS 10.0\)](#)

JoseMar - December 14, 2025, 9:19 pm

CRITICAL Apache Tika
XXE CVE-2025-66516 (CVSS 10.0)

What the hell happened

Apache Tika, yeah, that library a lot of us use without really thinking about it, just got slapped with a CVSS 10.0. Max score. Game over level stuff.

Here you have the short version, CVE-2025-66516 dropped, and it's a nasty XXE. We're talking XML External Entity injection through a crafted PDF with XFA inside. Yeah, a PDF. Not some weird edge-case format. It hits tika-core, tika-parser-pdf-module, and tika-parsers across a ton of versions, basically years of releases. There is a patch, but only if you actually move to 3.2.2 or 2.0.0 where it matters.

What really got me is that this isn't just "oh, update and move on." A lot of people upgraded only part of the stack, like the PDF parser, but left the core library untouched. Guess what, still vulnerable. Apparently this exact thing slipped through with the previous CVE too, CVE-2025-54988. So yeah, we've already been here, and somehow still tripped over it again.

Why this actually matters

XXE is no joke. File reads, possible RCE, depends how Tika is wired into your app. So yeah, if you're processing user uploads, resumes, invoices, random PDFs people throw at your app, I can already feel that little panic sweat kicking in.

Check your versions. Don't assume you're fine just because "we updated a while ago." If Tika is anywhere in your pipeline, ten minutes now is worth it.