Orfox Private Browser - Bug #8032
Crash in parser/renderer, hopefully without memory corruption? Orfox-1.2release

11/14/2016 06:14 pm - Anonymous

Status:	New	**Start date:**	10/01/2016
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	2.00 hours
Target version:			
Component:			

Description

*__*Steps to reproduce;
open https://play.google.com/store/apps/details?id=de.j4velin.wifiAutoOff with latest Orfox from F-Droid
Scroll up and down a dozen or so times. It will scroll very slowly like there was a ton of scripts running or something (it didn't do this in ESR38.1 without a ton of tabs open).
Crash

Notes;
Opening over 50 or tabs in the old version made it instable to the point where it would sometimes crash just while scrolling a page, but there were only a few tabs open, so it might have been memory exhaustion in the old ESR38.1, but it would be nice to know if there is remote code execution in the ESR45 just from normal browsing.
There was little to no CPU/net usage by anything else (in 38.1 and 45.4).

Configuration;
Plugins/media(except images); never load(because of stagefright 2.0)
javascript.enabled=false(since NoScript exempts all popular sites by default)
All autoupdate stuff in about:config disabled(since no word if pinning was fixed in fennec)
Everything else stock

Minidump/stacktrace/logcat;
Sorry, no.

Keep up the great work, this is all that's between humanity and total oppression.
Just confirming that this is merely DoS and not Itherwise exploitable would be a huge relief.
The 2 hour estimate is just to confirm that it's safe to browse with no javascript/plugins, not to fix the crash.

Related issues:

Copied from Orfox Private Browser - Bug # 7961: Crash in parser/renderer, hop...	**New**	**10/01/2016**