

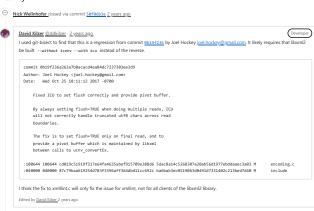
This is found by Agency for Defense Development (ADD).

① Drag your designs here or click to upload



Activity

◀



Joel Hockey @joel.hockey · 2 years ago
@ 0001-Validate-UTF8-in-xmlEncodeEntities.patch

Here is a patch to validate UTF-8 within xmlEncodeEntities and avoid buffer overflow. This should fix the issue for all clients of libxml2. I would be inclined to revert \$64663e so that further fuzzing in xmllint will catch any other errors inside libxml2.

My change in https://example.com/but/436 doesn't directly relate to this code, but I suspect that by fixing the handling of truncated UTF-8 in one place, it reveals errors in other places.

Edited by Joel Hockey 2 years ago

Nick Wellnhofer @nwellnhof · 2 years ago

I think this issue is really restricted to xmllint.



My change in https://de.org/linear-place, but I suspect that by fixing the handling of truncated UTF-8 in one place, it reveals errors in other places.

The commit probably just changed some boundaries of multi-byte characters. If the buffer in xmllint happens to end with a complete, untruncated UTF-8 sequence, the bug isn't triggered.

In general, libxml2 validates UTF-8 when parsing and then assumes that all UTF-8 is valid. But it's always a good idea to at least avoid undefined behavior with invalid UTF-8, so thanks for the patch.

Nick Wellnhofer @nwellnhof - 1 year ago
For the record, Joel's patch is now applied: bf227135

Nick Wellnhofer marked this issue as related to #235 (closed) 1 year ago

Doel Hockey mentioned in commit bf227135 1 year ago

Please register or sign in to reply