New issue

Buffer overflow in Expat.xs (patch) [rt.cpan.org #19860] #39

Closed #122

Labels Has Patch

toddr opened on Sep 24, 2019

Migrated from rt.cpan.org#19860 (status was 'new')

Requestors:

- rantwijk@science.uva.nl

Attachments:

- XML-Parser-2.34-stackoveflow.patch

From on 2006-06-13 09:26:38
:

```
While looking through the Expat.xs code, I noticed a potential heap
buffer overflow:

Expat.xs, line 498:
  if (cbv->st_serial_stackptr >= cbv->st_serial_stacksize) {
    unsigned int newsize = cbv->st_serial_stacksize + 512;
    Renew(cbv->st_serial_stack, newsize, unsigned int);
    cbv->st_serial_stacksize = newsize;
  }
  cbv->st_serial_stack[++cbv->st_serial_stackptr] =  cbv->st_serial;

Note that in the case (stackptr == stacksize - 1), the stack will NOT be
expanded. Then the new value will be written at location (++stackptr),
which equals stacksize and therefore falls just outside the allocated
buffer.

The bug can be observed using Valgrind when parsing an XML file with
```

```
very deep element nesting

A simple fix is to change the test to:
  if (cbv->st_serial_stackptr + 1 >= cbv->st_serial_stacksize) {

Package: XML-Parser-2.34
Perl version: v5.8.5 built for i386-linux-thread-multi
OS: Fedora Core release 3

Bye,
  Joris.
```

toddr on Sep 24, 2019 Member Author

```
diff -urN -U 5 XML-Parser-2.34.orig/Expat/Expat.xs XML-Parser-2.34/Expat/Expat.xs
--- XML-Parser-2.34.orig/Expat/Expat.xs 2003-07-28 16:41:10.000000000 +0200
+++ XML-Parser-2.34/Expat/Expat.xs  2006-06-13 11:23:40.000000000 +0200
@@ -493,11 +493,11 @@
       resume_callbacks(cbv);
       cbv->skip_until = 0;
     }
   }

-  if (cbv->st_serial_stackptr >= cbv->st_serial_stacksize) {
+  if (cbv->st_serial_stackptr + 1 >= cbv->st_serial_stacksize) {
     unsigned int newsize = cbv->st_serial_stacksize + 512;

     Renew(cbv->st_serial_stack, newsize, unsigned int);
     cbv->st_serial_stacksize = newsize;
   }
```

toddr added **Has Patch** on Sep 24, 2019

toddr-bot added a commit that references this issue 2 weeks ago

`fix: off-by-one heap buffer overflow in st_serial_stack growth check` ···

`08dd37c`

toddr-bot mentioned this 2 weeks ago

fix: off-by-one heap buffer overflow in st_serial_stack #122

toddr closed this as completed in #122 2 weeks ago

hartwork last week

This seems to be CVE-2006-10003.

👍 1

Metadata

Assignees

No one assigned

Labels

Has Patch

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests