The Fuzzing Project

Blog and Advisories

Heap Overflow in PCRE

Posted by Hanno Böck on Tuesday, November 24. 2015

The Perl Compatible Regular Expressions (PCRE) library has just released a new version which fixes a number of security issues.

Fuzzing the pcretest tool uncovered an input leading to a heap overflow in the function pcre_exec. This bug was found with the help of american fuzzy lop and address sanitizer.
Upstream bug #1637

This is fixed in PCRE 8.38. There are two variants of PCRE, the classic one and PCRE2. PCRE2 is not affected.

Appart from that a couple of other vulnerabilities found by other people have been fixed in this release:
Stack overflow in compile_regex (bug #1503)
Heap overflow in compile_regex (bug #1672)
Stack overflow in compile_regex (bug #1515)
Heap overflow in compile_regex (bug #1636, CVE-2015-3210)
Stack overflow in match (bug #1638, CVE-2015-3217)
Heap overflow in compile_regex (bug #1667)
(this list may be incomplete)

If you use PCRE with potentially untrusted regular expressions you should update immediately. There is no immediate risk if you use regular expressions from a trusted source with an untrusted input.

Trackbacks

No Trackbacks

Comments

No comments