Security Research Advisory

Ruby *rb_ary_fill()*

Denial of Service

Table of Contents

Denial of Service					Advisory Number
					SN-08-02
Severity	Software	Version(s)	Accessibility	CVE	Author(s)
M	Ruby	1.8.x 1.9.x	Local/ Remote	-	Vincenzo Iozzo
	Vendor URL		Advisory URL		
	http://www.ruby-lang.org/		-		

Date	Details
23/06/2008	Vendor disclosure
25/06/2008	Vendor acknowledgment
25/06/2008	Patch release
30/06/2008	Public disclosure

Summary

Ruby is an interpreted language, used in a wide range of applications. The specific issue is a Denial of Service vulnerability, caused by an integer overflow.

Fix: http://svn.ruby-lang.org/cgi-bin/viewvc.cgi/trunk/array.c?view=markup.

Vulnerability Details

An integer overflow vulnerability in *rb_ary_fill()* can lead to denial of service. On Ruby on Rails, an attacker may craft specific requests and by XSS (for example) can cause a legitimate user to crash the web server. However, it doesn't allow arbitrary code execution.

Technical Details

Description

The vulnerability was found in *rb_ary_fill()*. The *len* variable value, as shown in the source code paragraph, is incremented by one in a previous function and it is specified by the user. The lack of sanity check on the input, leads to an integer overflow here:

```
REALLOC_N(RARRAY(ary)->ptr, VALUE, end);
```

This macro, in fact, will allocate *end * VALUE*. On 32bit architectures VALUE is 4. If an attacker specifies a value of *0x3fffffff*, this macro will allocate a memory region of 0, so that next time *ary->ptr* is accessed, it will raise a SIGSEGV (NULL referencing). A simple exploit can be the following.

PoC Exploit:

```
a = []
a.fill("A",0..0x3fffffff)
```

Vulnerable Code

Function: *rb_ary_modify()*

```
rb_ary_modify(ary);
    end = beg + len;
    if (end < 0) {
    rb_raise(rb_eArgError, "argument too big");
    }
    if (end > RARRAY(ary)->len) {
    if (end >= RARRAY(ary)->aux.capa) {
        REALLOC_N(RARRAY(ary)->ptr, VALUE, end);
        RARRAY(ary)->aux.capa = end;
    }
```

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41