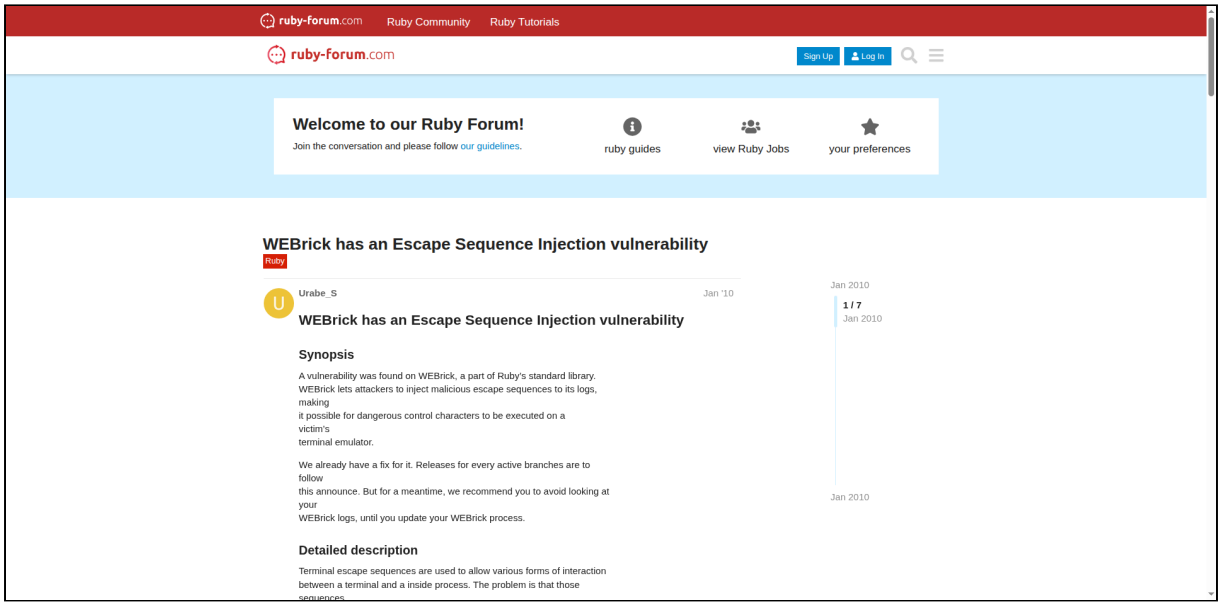
PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Page Screenshot



WEBrick has an Escape Sequence Injection vulnerability

Urabe_S **Jan '10**

WEBrick has an Escape Sequence Injection vulnerability

Synopsis

A vulnerability was found on WEBrick, a part of Ruby's standard library. WEBrick lets attackers to inject malicious escape sequences to its logs, making
it possible for dangerous control characters to be executed on a victim's
terminal emulator.

We already have a fix for it. Releases for every active branches are to follow
this announce. But for a meantime, we recommend you to avoid looking at your
WEBrick logs, until you update your WEBrick process.

Detailed description

Terminal escape sequences are used to allow various forms of interaction between a terminal and a inside process. The problem is that those sequences
are not intended to be issued by untrusted sources; such as network inputs. So
if a remote attacker could inject escape sequences into WEBrick logs, and a
victim happen to consult them through his/her terminal, the attacker could take
advantages of various weaknesses in terminal emulators[1].

And WEBrick fails to filter those terminal escape sequences.

Example:

```
% xterm -e ruby -rwebrick -e
```

'WEBrick::HTTPServer.new(:Port=>8080).start' &
% wget **http://localhost:8080/]2%3Bowned**

Watch out for the window title of xterm.

Affected versions

- Ruby 1.8.6 patchlevel 383 and all prior versions
- Ruby 1.8.7 patchlevel 248 and all prior versions
- Development versions of Ruby 1.8 (1.8.8dev)
- Ruby 1.9.1 patchlevel 376 and all prior versions
- Development versions of Ruby 1.9 (1.9.2dev)

Solutions

- Fixes for 1.8.6, 1.8.7, and 1.9.1 are to follow this announce.
- For development versions, please update to the most recent revision for each
  development branch.

Credit

Credit to Giovanni "evilaliv3" Pellerano, Alessandro "jekil" Tanasi, and Francesco "ascii" Ongaro for discovering this vulnerability.

[1] **'Terminal Emulator Security Issues' - MARC**
"Terminal Emulator Security Issues"

Urabe S. wrote:

> - Fixes for 1.8.6, 1.8.7, and 1.9.1 are to follow this announce.

This is it. The only change since pl. 248 is the fix for this issue.

- **ftp://ftp.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.tar.gz**
- **ftp://ftp.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.tar.bz2**
- **ftp://ftp.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.zip**

Checksums:

```
MD5(ruby-1.8.7-p249.tar.gz)= d7db7763cffad279952eb7e9bbfc221c
SHA256(ruby-1.8.7-p249.tar.gz)=
```

a969f5ec00f096f01650bfa594bc408f2e5cfc3de21b533ab62b4f29eb8ca653
SIZE(ruby-1.8.7-p249.tar.gz)= 4831548

```
MD5(ruby-1.8.7-p249.tar.bz2)= 37200cc956a16996bbfd25bb4068f242
SHA256(ruby-1.8.7-p249.tar.bz2)=
```

8b89448fc79df6862660e9f77e884f06c76da28f078d8edd2f17567a615f3af5
SIZE(ruby-1.8.7-p249.tar.bz2)= 4153461

```
MD5(ruby-1.8.7-p249.zip)= 46d62547093648a2e8a3d934c5140175
SHA256(ruby-1.8.7-p249.zip)=
```

8e58812bef5360309c2bf1fe005d3673189367f6ba655b3d7e97fd0d415d3467
SIZE(ruby-1.8.7-p249.zip)= 5890216

Thanks.

Urabe_S **Jan '10**

On Sun, Jan 10, 2010 at 5:43 AM, Urabe S. **removed_email_address@domain.invalid** wrote:

> Urabe S. wrote:
>
> > - Fixes for 1.8.6, 1.8.7, and 1.9.1 are to follow this announce.
>
> This is it. The only change since pl. 248 is the fix for this issue.

Based only on the timing, I'm assuming that 'this issue' is the
webrick vulnerability. Yes?

–
Rick DeNatale

Blog: **http://talklikeaduck.denhaven2.com/**
Twitter: **http://twitter.com/RickDeNatale**
WWR: **http://www.workingwithrails.com/person/9021-rick-denatale**
LinkedIn: **Rick DeNatale - Developer - IBM | LinkedIn**