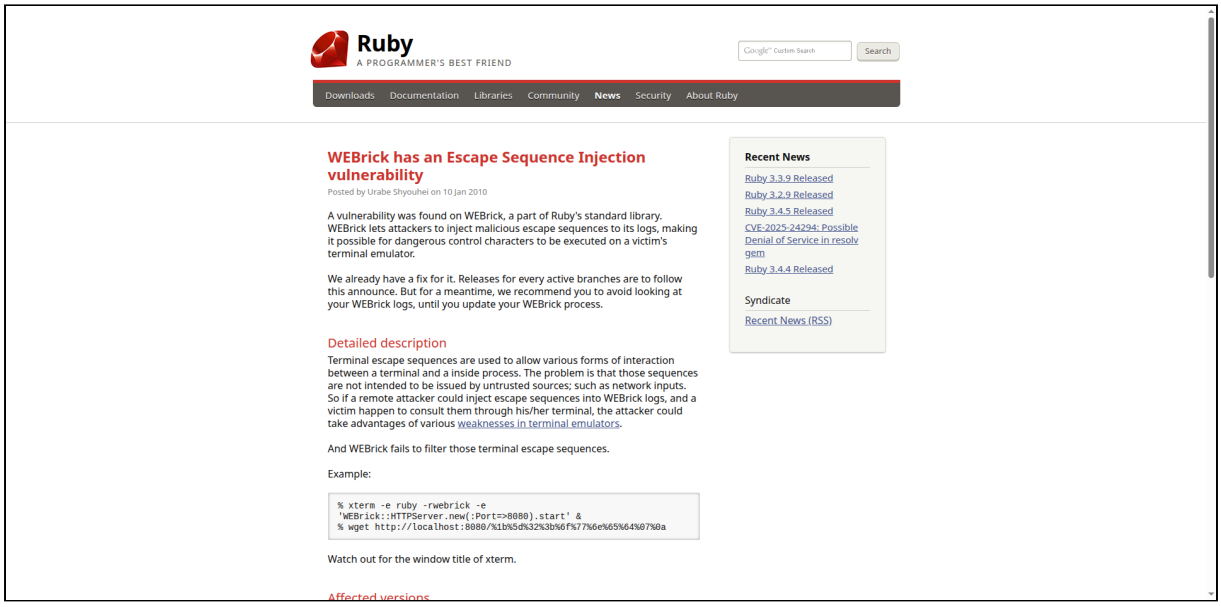
PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Page Screenshot



WEBrick has an Escape Sequence Injection vulnerability

Posted by Urabe Shyouhei on 10 Jan 2010

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.

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/%1b%5d%32%3b%6f%77%6e%65%64%07%0a
```

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.
  - **Update** 1.8.7 pl. 249 was released to fix this issue. 1.8.7 users are encouraged to upgrade.
    - https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.tar.gz
    - https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.tar.bz2
    - https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.7-p249.zip
  - **Update** 1.9.1 pl. 378 was released to fix this issue. 1.9.1 users are encouraged to upgrade.
    - https://cache.ruby-lang.org/pub/ruby/1.9/ruby-1.9.1-p378.tar.gz
    - https://cache.ruby-lang.org/pub/ruby/1.9/ruby-1.9.1-p378.tar.bz2
    - https://cache.ruby-lang.org/pub/ruby/1.9/ruby-1.9.1-p378.zip
  - **Update** 1.8.6 pl. 388 was released to fix this issue. 1.8.6 users are encouraged to upgrade.
    - https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.6-p388.tar.gz

Recent News

Ruby 3.3.9 Released
Ruby 3.2.9 Released
Ruby 3.4.5 Released
CVE-2025-24294: Possible Denial of Service in resolv gem
Ruby 3.4.4 Released

Syndicate

Recent News (RSS)

    - https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.6-p388.tar.bz2
    - https://cache.ruby-lang.org/pub/ruby/1.8/ruby-1.8.6-p388.zip
- 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.