Ruby

A PROGRAMMER'S BEST FRIEND

CVE-2017-17405: Command injection vulnerability in Net::FTP

Posted by nagachika on 14 Dec 2017

There is a command injection vulnerability in Net::FTP bundled with Ruby. This vulnerability has been assigned the CVE identifier CVE-2017-17405.

Details

`Net::FTP#get`, `getbinaryfile`, `gettextfile`, `put`, `putbinaryfile`, and `puttextfile` use `Kernel#open` to open a local file. If the `localfile` argument starts with the pipe character `"|"`, the command following the pipe character is executed. The default value of `localfile` is `File.basename(remotefile)`, so malicious FTP servers could cause arbitrary command execution.

All users running an affected release should upgrade immediately.

Affected Versions

- Ruby 2.2 series: 2.2.8 and earlier
- Ruby 2.3 series: 2.3.5 and earlier
- Ruby 2.4 series: 2.4.2 and earlier
- Ruby 2.5 series: 2.5.0-preview1
- prior to trunk revision r61242

Credit

Thanks to Etienne Stalmans from the Heroku product security team for reporting the issue.

History

- Originally published at 2017-12-14 16:00:00 (UTC)

This site in other languages: Български, Deutsch, English, Español, Français, Bahasa Indonesia, Italiano, 日本語, 한국어, polski, Português, Русский, Türkçe, Tiếng Việt, 简体中文, 繁體中文.

This website is proudly maintained by members of the Ruby community.