USN-3685-2: Ruby regression

USN-3685-1 fixed a vulnerability in Ruby. The fix for CVE-2017-0903 introduced
a regression in Ruby. This update fixes the problem.
Original advisory details:

Some of these CVE were already addressed in previous
USN: 3439-1, 3553-1, 3528-1. Here we address for
the remain releases.

It was discovered that Ruby incorrectly handled certain inputs.
An attacker could use this to cause a buffer overrun.
(CVE-2017-0898)

It was discovered that Ruby incorrectly handled certain files.
An attacker could use this to overwrite any file on the filesystem.
(CVE-2017-0901)

It was discovered that Ruby was vulnerable to a DNS hijacking vulnerability.
An attacker could use this to possibly force the RubyGems client to download
and install gems from a server that the attacker controls.
(CVE-2017-0902)

It was discovered that Ruby incorrectly handled certain YAML files.
An attacker could use this to possibly execute arbitrary code.
(CVE-2017-0903)

It was discovered that Ruby incorrectly handled certain files.
An attacker could use this to expose sensitive information.
(CVE-2017-14064)

It was discovered that Ruby incorrectly handled certain inputs.

An attacker could use this to execute arbitrary code. (CVE-2017-10784)

It was discovered that Ruby incorrectly handled certain network requests.
An attacker could possibly use this to inject a crafted key into a HTTP
response. (CVE-2017-17742)

It was discovered that Ruby incorrectly handled certain files. An attacker could possibly use this to execute arbitrary code. This update is only addressed to ruby2.0. (CVE-2018-1000074)

It was discovered that Ruby incorrectly handled certain network requests.
An attacker could possibly use this to cause a denial of service.
(CVE-2018-8777)