

Alpine Linux - Bug #9541

Bug # 9511 (Resolved): Git RCE vulnerability regarding submodules (CVE-2018-17456)

[3.8] Git RCE vulnerability regarding submodules (CVE-2018-17456)

10/09/2018 07:58 AM - Alichia CH

Status: Closed	Start date: 10/07/2018
Priority: Normal	Due date:
Assignee: Natanael Copa	% Done: 100%
Category: Security	Estimated time: 0.00 hour
Target version: 3.8.2	Security IDs:
Affected versions:	

Description

Git before 2.14.5, 2.15.x before 2.15.3, 2.16.x before 2.16.5, 2.17.x before 2.17.2, 2.18.x before 2.18.1, and 2.19.x before 2.19.1 allows remote code execution during processing of a recursive "git clone" of a superproject if a .gitmodules file has a URL field beginning with a '-' character.

References:

<https://www.openwall.com/lists/oss-security/2018/10/06/3>
<https://nvd.nist.gov/vuln/detail/CVE-2018-17456>

Patches:

<https://github.com/git/git/commit/98afac7a7cefdca0d2c4917dd8066a59f7088265>
<https://github.com/git/git/commit/f6adec4e329ef0e25e14c63b735a5956dc67b8bc>
<https://github.com/git/git/commit/273c61496f88c6495b886acb1041fe57965151da>

For the fsck check:
<https://github.com/git/git/commit/a124133e1e6ab5c7a9fef6d0e6bcb084e3455b46>
<https://github.com/git/git/commit/1a7fd1fb2998002da6e9ff2ee46e1bdd25ee8404>

Associated revisions

Revision 898a0bb2 - 10/24/2018 05:12 PM - Natanael Copa

main/git: security upgrade to 2.18.1 (CVE-2018-17456)

fixes #9541

History

#1 - 10/24/2018 05:13 PM - Natanael Copa

- Status changed from New to Resolved
- % Done changed from 0 to 100

Applied in changeset [alpine:898a0bb28afee2d77234bbbf3bd75380c9bb529c](https://git.alpinelinux.org/?id=alpine:898a0bb28afee2d77234bbbf3bd75380c9bb529c).

#2 - 10/25/2018 08:13 AM - Alichia CH

- Project changed from Alpine Security to Alpine Linux
- Category set to Security
- Status changed from Resolved to Closed
- Security IDs deleted (CVE-2018-17456)