

Alpine Linux - Bug #6762

Bug # 6761 (Closed): borgbackup: multiple vulnerabilities (CVE-2016-10099, CVE-2016-10100)

[3.5] borgbackup: multiple vulnerabilities (CVE-2016-10099, CVE-2016-10100)

01/27/2017 10:47 AM - Alichia CH

| | |
|------------------------------|----------------------------------|
| Status: Closed | Start date: 01/27/2017 |
| Priority: Normal | Due date: |
| Assignee: | % Done: 100% |
| Category: Security | Estimated time: 0.00 hour |
| Target version: 3.5.2 | Security IDs: |
| Affected versions: | |

Description

CVE-2016-10099:

Borg (aka BorgBackup) before 1.0.9 has a flaw in the cryptographic protocol used to authenticate the manifest (list of archives), potentially allowing an attacker to spoof the list of archives.

References:

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10099>
<http://borgbackup.readthedocs.io/en/stable/changes.html#pre-1-0-9-manifest-spoofing-vulnerability>

CVE-2016-10100:

Borg (aka BorgBackup) before 1.0.9 has a flaw in the way duplicate archive names were processed during manifest recovery, potentially allowing an attacker to overwrite an archive.

References:

<http://borgbackup.readthedocs.io/en/stable/changes.html#pre-1-0-9-manifest-spoofing-vulnerability>
<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10100>

Associated revisions

Revision 97880036 - 01/27/2017 11:01 AM - Natanael Copa

community/borgbackup: security upgrade to 1.0.9 (CVE-2016-10099,CVE-2016-10100)

fixes #6762

History

#1 - 01/27/2017 11:01 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset [alpine:978800365815537d1a1e289d239d6a316bf70455](https://git.alpinelinux.org/cgit/alpine/?id=978800365815537d1a1e289d239d6a316bf70455).

#2 - 01/27/2017 11:03 AM - Alichia CH

- Category set to Security

- Status changed from Resolved to Closed