

## Alpine Linux - Bug #9669

Bug # 9667 (Closed): cabextract: Buffer overflow (CVE-2018-18584)

### [3.8] cabextract: Buffer overflow (CVE-2018-18584)

11/21/2018 11:40 AM - Alichia CH

<b>Status:</b> Closed	<b>Start date:</b> 11/21/2018
<b>Priority:</b> Normal	<b>Due date:</b>
<b>Assignee:</b> Leonardo Arena	<b>% Done:</b> 100%
<b>Category:</b> Security	<b>Estimated time:</b> 0.00 hour
<b>Target version:</b> 3.8.2	<b>Security IDs:</b> CVE-2018-18584
<b>Affected versions:</b>	
<b>Description</b> cabextract before 1.8, the CAB block input buffer is one byte too small for the maximal Quantum block, leading to an out-of-bounds write.	
<b>Fixed In Version:</b>  cabextract 1.8	
<b>References:</b>  <a href="https://www.cabextract.org.uk">https://www.cabextract.org.uk</a> <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18584">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18584</a> <a href="https://www.openwall.com/lists/oss-security/2018/10/22/1">https://www.openwall.com/lists/oss-security/2018/10/22/1</a>	

#### History

##### #1 - 11/27/2018 03:45 PM - Natanael Copa

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

fixed in [alpine:4edf9b0a6836a75eaabe7e1f1cbd0c0238cb15f0](https://github.com/lcamtuf/cabextract/commit/4edf9b0a6836a75eaabe7e1f1cbd0c0238cb15f0)

##### #2 - 11/28/2018 07:10 AM - Alichia CH

- Project changed from Alpine Security to Alpine Linux
- Category set to Security
- Status changed from Resolved to Closed