

Alpine Linux - Bug #7439

libsndfile: Multiple vulnerabilities (CVE-2017-8361, CVE-2017-8362, CVE-2017-8363, CVE-2017-8365)

06/16/2017 09:03 AM - Alichia CH

Status:	Closed	Start date:	06/16/2017
Priority:	Normal	Due date:	
Assignee:	Natanael Copa	% Done:	100%
Category:	Security	Estimated time:	0.00 hour
Target version:		Security IDs:	
Affected versions:			
Description			
CVE-2017-8361: The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file.			
Reference:			
http://openwall.com/lists/oss-security/2017/05/01/1			
Patch:			
https://github.com/erikd/libsndfile/commit/fd0484aba8e51d16af1e3a880f9b8b857b385eb3			
CVE-2017-8362: The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted audio file.			
Reference:			
http://openwall.com/lists/oss-security/2017/05/01/2			
Patch:			
https://github.com/erikd/libsndfile/commit/ef1dbb2df1c0e741486646de40bd638a9c4cd808			
CVE-2017-8363: The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file.			
Reference:			
http://openwall.com/lists/oss-security/2017/05/01/3			
Patch:			
https://github.com/erikd/libsndfile/commit/fd0484aba8e51d16af1e3a880f9b8b857b385eb3			
CVE-2017-8365: The i2les_array function in pcm.c in libsndfile allows attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file.			
Affected version:			
1.0.28			
Reference:			
http://openwall.com/lists/oss-security/2017/05/01/5			
Patch:			
https://github.com/erikd/libsndfile/commit/fd0484aba8e51d16af1e3a880f9b8b857b385eb3			
Subtasks:			

Bug # 7440: [3.7] libsndfile: Multiple vulnerabilities (CVE-2017-8361, CVE-2017-8362, C...	Closed
Bug # 7441: [3.6] libsndfile: Multiple vulnerabilities (CVE-2017-8361, CVE-2017-8362, C...	Closed
Bug # 7442: [3.5] libsndfile: Multiple vulnerabilities (CVE-2017-8361, CVE-2017-8362, C...	Closed
Bug # 7443: [3.4] libsndfile: Multiple vulnerabilities (CVE-2017-8361, CVE-2017-8362, C...	Closed
Bug # 7444: [3.3] libsndfile: Multiple vulnerabilities (CVE-2017-8361, CVE-2017-8362, C...	Closed

History

#1 - 07/05/2017 08:27 AM - Alicha CH

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