



CVE-2017-5834

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-5834
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-03 15:59:00 UTC
Updated	2017-03-07 02:59:00 UTC
Description	The parse_dict_node function in bplist.c in libplist allows attackers to cause a denial of service (out-of-bounds heap read and

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libimobiledevice	Libplist	All	All	All	All
Application	Libimobiledevice	Libplist	All	All	All	All

References

Reference	Source	Link	Tags
libplist Multiple Local Heap Buffer Overflow and Denial-of-Service Vulnerabilities	BID	www.securityfocus.com	
oss-security - CVE request: multiples vulnerabilities in libplist	MLIST	www.openwall.com	Mailing List, P
oss-security - Re: CVE request: multiples vulnerabilities in libplist	MLIST	www.openwall.com	Mailing List, P
[SECURITY] [DLA 2168-1] libplist security update	MLIST	lists.debian.org	
heap-buffer-overflow in parse_dict_node · Issue #89 · libimobiledevice/libplist · GitHub	CONFIRM	github.com	Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[671068](#) EulerOS Security Update for libplist (EulerOS-SA-2019-2613)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)