



CVE-2017-5545

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

Summary

CVE	CVE-2017-5545
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-21 01:59:00 UTC
Updated	2020-04-02 10:15:00 UTC
Description	The main function in plistutil.c in libimobiledevice libplist through 1.12 allows attackers to obtain sensitive information from p

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

References

Reference
Libimobiledevice Libplist 'plistutil.c' Heap Buffer Overflow Vulnerability
[SECURITY] [DLA 2168-1] libplist security update
AddressSanitizer: heap-buffer-overflow on address 0xb5e007d7 at pc 0x804a78c bp 0xbf815888 sp 0xbf81587c · Issue #87 · libimobiledevice
plistutil: Prevent OOB heap buffer read by checking input size · libimobiledevice/libplist@7391a50 · GitHub
CVE Program record
NVD vulnerability detail

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](#)