



CVE-2016-6547

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

Summary

CVE	CVE-2016-6547
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-13 20:29:00 UTC
Updated	2019-10-09 23:19:00 UTC
Description	The Zizai Tech Nut mobile app stores the account password used to authenticate to the cloud API in cleartext in the cache.

Risk And Classification

Problem Types: CWE-255 | CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nutspace	Nut Mobile	-	All	All	All
Application	Nutspace	Nut Mobile	-	All	All	All

References

Reference	Source	Link	Tags
Zizai Tech Nut Multiple Security Vulnerabilities	BID	www.securityfocus.com	Third Party Advisory,
Multiple Bluetooth Low Energy (BLE) Tracker Vulnerabilities	MISC	blog.rapid7.com	Exploit, Third Party A
Vulnerability Note VU#402847 - Zizai Tech Nut contains multiple vulnerabilities	CERT-VN	www.kb.cert.org	Third Party Advisory,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks to Deral Heiland and Adam Compton of Rapid7, Inc. for reporting this vulnerability.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)