

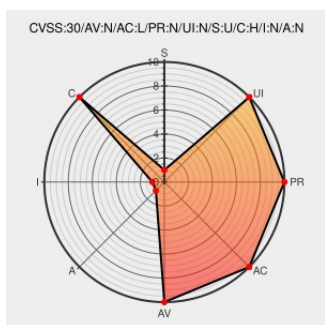


CVE-2019-5927

Published on: 03/27/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:59 PM UTC

CVE-2019-5927

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [An](#) from [Weban](#) contain the following vulnerability:

Directory traversal vulnerability in 'an' App for iOS Version 3.2.0 and earlier allows remote attackers to read arbitrary files via unspecified vectors.

CVE-2019-5927 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [PERSOL CAREER CO., LTD.](#) - 'an' App for iOS version **Version 3.2.0 and earlier**

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
バイトアプリ「an」iPhone、Android版 バイト探しはan (アン)	Product Vendor Advisory web.archive.org	MISC weban.jp/contents/c/smartphone_apri/

Not Archived

jvn.jp/en/jp/JVN60497148/index.html

There are currently no QIDs associated with this CVE

Next ID→

CVE.report and Source URL Uptime Status status.cve.report