



CVE-2020-11882

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

Summary

CVE	CVE-2020-11882
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-07 16:15:00 UTC
Updated	2020-07-15 17:58:00 UTC
Description	The O2 Business application 1.2.0 for Android exposes the canvasm.myo2.SplashActivity activity to other applications. The

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Telefonica	O2 Business	1.2.0	All	All	All
Application	Telefonica	O2 Business	1.2.0	All	All	All

References

Reference	Source	Link	Tags
Android o2 Business 1.2.0 Open Redirect ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Advisory, VDB Entry
rcesecurity.com	MISC	rcesecurity.com	Broken Link
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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