



CVE-2015-9232

Published on: 09/20/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

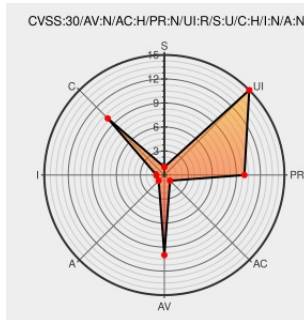
CVE-2015-9232

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Good For Enterprise](#) from [Good](#) contain the following vulnerability:

The Good for Enterprise application 3.0.0.415 for Android does not use signature protection for its Authentication Delegation API intent. Also, the Good Dynamic application activation process does not attempt to detect malicious activation attempts involving modified names beginning with a com.good.gdgma substring. Consequently, an

attacker could obtain access to intranet data. This issue is only relevant in cases where the user has already downloaded a malicious Android application.

CVE-2015-9232 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **2.6 - LOW**

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

CVE References

Description	Tags	Link
	Exploit	MISC: www.madgag.ch/editions/M7_15_03_GOOD_Auth_Delegation.txt

Exploit
Mitigation
Third Party Advisory
www.modzero.ch
text/plain

MISC www.modzero.ch/advisories/MZ-15-03-GOOD-Auth-Delegation.txt

SecurityFocus

Exploit
Mitigation
Third Party Advisory
VDB Entry
www.securityfocus.com
text/html

MISC www.securityfocus.com/archive/1/536543

BlackBerry
Support

Third Party Advisory
community.blackberry.com
text/html

MISC community.blackberry.com/community/blogs/blog/2015/10/02/what-you-need-to-know-modzero-insecure-application-coupling

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Good	Good For Enterprise	3.0.0.415	All	All	All
Application	Good	Good For Enterprise	3.0.0.415	All	All	All
cpe:2.3:a:good:good_for_enterprise:3.0.0.415:*:*:*:android:*:*						
cpe:2.3:a:good:good_for_enterprise:3.0.0.415:*:*:*:android:*:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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