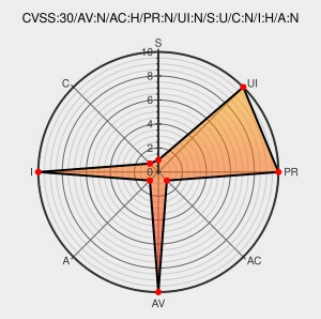
CVE-2015-2674

Published on: 08/09/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:19 PM UTC

CVE-2015-2674

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Restkit from Restkit contain the following vulnerability:

Restkit allows man-in-the-middle attackers to spoof TLS servers by leveraging use of the ssl.wrap_socket function in Python with the default CERT_NONE value for the cert_reqs argument.

CVE-2015-2674 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - Re: Assign a CVE for Python's restkit Please	Mailing List VDB Entry www.openwall.com text/html	MLIST [oss-security] 20150323 Re: Assign a CVE for Python's restkit Please

Doesn't Validate TLS · Issue #140 · benoitc/restkit · GitHub	Third Party Advisory github.com text/html	MISC github.com/benoitc/restkit/issues/140
Bug 1202837 – CVE-2015-2674 python-restkit: incorrect SSL/TLS certificate validation	Issue Tracking Third Party Advisory VDB Entry bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1202837

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	Restkit	Restkit	-	All	All	All
Application	Restkit	Restkit	-	All	All	All

cpe:2.3:a:restkit:restkit:-:*:*:*:*:*:*:*:

cpe:2.3:a:restkit:restkit:-:*:*:*:*:*:*:*:

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 registred 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.

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