



CVE-2017-8342

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

Summary

CVE	CVE-2017-8342
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-30 15:59:00 UTC
Updated	2020-04-25 23:15:00 UTC
Description	Radicale before 1.1.2 and 2.x before 2.0.0rc2 is prone to timing oracles and simple brute-force attacks when using the httpa

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Radicale	Radicale	2.0.0	rc1	All	All
Application	Radicale	Radicale	2.0.0	rc1	All	All
Application	Radicale	Radicale	All	All	All	All

References

Reference	Source
Random timer to avoid timing oracles and simple bruteforce attacks · Kozzea/Radicale@190b1dd · GitHub	CONF
Random timer to avoid timing oracles and simple bruteforce attacks · Kozzea/Radicale@059ba8d · GitHub	CONF
#861514 - radicale: CVE-2017-8342: htpasswd authentication vulnerable to timing-based bruteforce attacks - Debian Bug report logs	CONF
Radicale/NEWS.rst at 1.1.2 · Kozzea/Radicale · GitHub	CONF
[SECURITY] [DLA 2187-1] radicale security update	MLIST
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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](#)