



CVE-2014-1604

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2014-1604
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-28 00:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	The parser cache functionality in parsergenerator.py in RPLY (aka python-rply) before 0.7.1 allows local users to spoof each

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python	Rply	All	All	All	All

References

Reference	Source	Link
#735263 - python-rply: CVE-2014-1604: insecure use of /tmp - Debian Bug report logs	CONFIRM	bugs.debian.org
102202	OSVDB	www.osvdb.com
oss-security - Fwd: [Python-modules-team] Bug#735263: python-rply: insecure use of /tmp	MLIST	www.openwall.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
The parser cache is now always handled in a per-user fashion. · alex/rply@fc9bbcd · GitHub	CONFIRM	github.com
Security Advisory SA56429 - Python RPLY Module Insecure Temporary Files Handling Security Issue - Secunia	SECUNIA	secunia.com
oss-security - Re: Fwd: [Python-modules-team] Bug#735263: python-rply: insecure use of /tmp	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)