CVE-2014-1604

MITRE | NVD | CVE.ORG | Print: PDF

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 cach

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.(
102202	OSVDB	www.osvdb.c
oss-security - Fwd: [Python-modules-team] Bug#735263: python-rply: insecure use of /tmp	MLIST	www.openwa
IBM X-Force Exchange	XF	exchange.xfc
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.openwa
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

994911 Python (Pip) Security Update for RPLY (GHSA-9gcf-pq99-rjw3)