



CVE-2013-0294

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

Summary

CVE	CVE-2013-0294
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-28 16:15:00 UTC
Updated	2020-01-31 19:07:00 UTC
Description	packet.py in pyrad before 2.1 uses weak random numbers to generate RADIUS authenticators and hash passwords, which

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	18	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	18	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Application	Pyrad Project	Pyrad	All	All	All	All
Application	Pyrad Project	Pyrad	All	All	All	All

References

Reference	Source
oss-security - Re: CVE request: python-pyrad insecurities	MISC
[SECURITY] Fedora 18 Update: python-pyrad-2.0-3.fc18	CONF
[SECURITY] Fedora 20 Update: python-pyrad-2.0-3.fc20	CONF
[SECURITY] Fedora 19 Update: python-pyrad-2.0-3.fc19	CONF
Use a better random generator. · pyradius/pyrad@38f74b3 · GitHub	CONF
IBM X-Force Exchange	MISC

911682 – (CVE-2013-0294) CVE-2013-0294 python-pyrad: poor randomness leads to predictable password hashing and RADIUS IDs	CON
pyrad Password Hash Information Disclosure Vulnerability and Packet Spoofing Vulnerability	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
Legacy QID Mappings 690232 Free Berkeley Software Distribution (FreeBSD) Security Update for pyrad (17702e54-3da0-11ec-b7e0-3085a9a95629) 997637 Python (Pip) Security Update for pyrad (GHSA-q4v3-wmm6-hcrx)	

© [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](#)