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	Sour
oss-security - Re: CVE request: python-pyrad insecurities	MISC
[SECURITY] Fedora 18 Update: python-pyrad-2.0-3.fc18	CON
[SECURITY] Fedora 20 Update: python-pyrad-2.0-3.fc20	CON
[SECURITY] Fedora 19 Update: python-pyrad-2.0-3.fc19	CON
Use a better random generator. · pyradius/pyrad@38f74b3 · GitHub	CON
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)

Free CVE JSON API cve.report/api

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