CVE-2008-0299

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2008-0299
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-16 23:00:00 UTC
Updated	2017-08-08 01:29:00 UTC
Description	common.py in Paramiko 1.7.1 and earlier, when using threads or forked processes, does not properly use RandomPool, wh

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Python Software Foundation	Paramiko	1.7.1	All	All	All
Application	Python Software Foundation	Paramiko	1.7.1	All	All	All

References

Reference	Source
403 Forbidden	MISC
Paramiko: Information disclosure — Gentoo Linux Documentation	GENTOO
paramiko Random Number Generator Weakness	BID
IBM X-Force Exchange	XF
[paramiko] [MERGE] insecure use of RandomPool	MISC
paramiko "RandomPool" Insecure Random Number Generator - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
[SECURITY] Fedora 8 Update: python-paramiko-1.7.1-3.fc8	FEDORA
#460706 - python-paramiko: CVE-2008-0299 insecure use of RandomPool - Debian Bug report logs	CONFIRM
Fedora update for python-paramiko - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
[SECURITY] Fedora 7 Update: python-paramiko-1.7.1-3.fc7	FEDORA
428727 – (CVE-2008-0299) CVE-2008-0299 Paramiko insecure use of RandomPool	CONFIRM
Gentoo update for paramiko - Advisories - Secunia	SECUNIA

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

997214 Python (Pip) Security Update for paramiko (GHSA-wqmm-q65g-2hqr)