



CVE-2000-0445

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2000-0445
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-05-24 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The pgpk command in PGP 5.x on Unix systems uses an insufficiently random data source for non-interactive key pair generation.

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:N/A:N

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pgp	Pgp	5.0i	All	All	All

Application	Pgp	Pgp	5.0_linux	All	All	All
Application	Pgp	Pgp	6.5_linux	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference	Source			Link		
www.osvdb.org/1355	af854a3a-2127-422b-91ae-364da2661108			www.osvdb.org		
archives.neohapsis.com/archives/bugtraq/2000-05/0273.html	af854a3a-2127-422b-91ae-364da2661108			archives.neohapsis.com/archives/bugtraq/2000-05/0273.html		
Multiple Vendor PGP5 Automatic Key Generation Routine Vulnerability	af854a3a-2127-422b-91ae-364da2661108			www.securityfocus.com		
CERT Advisory CA-2000-09 Flaw in PGP 5.0 Key Generation	af854a3a-2127-422b-91ae-364da2661108			www.cert.org		
CVE Program record	CVE.ORG			www.cve.org		
NVD vulnerability detail	NVD			nvd.nist.gov		

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.