CVE-2000-0678

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

Summary

CVE	CVE-2000-0678
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2000-10-20 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	PGP 5.5.x through 6.5.3 does not properly check if an Additional Decryption Key (ADK) is stored in the signed portion of a p

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/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	5.5.3i	All	All	All

Application	Pgp	Pgp	6.5.1i	All	All	All
Application	Pgp	Pgp	6.5.3i	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/4354	af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org
PGP ADK Insertion Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfo
CERT Advisory CA-2000-18 PGP May Encrypt Data With Unauthorized ADKs	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.