CVE-2005-0366

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

Summary

CVE	CVE-2005-0366
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The integrity check feature in OpenPGP, when handling a message that was encrypted using cipher feedback (CFB) mode.

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: CWE-326 | 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	Gnupg	Gnupg	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
OpenPGP Cipher Feedback Mode Chosen-Ciphertext Partial Plaintext Retrieval Vulnerability	af854a3a-2127-422b-91ae-364da26
www.osvdb.org/13775	af854a3a-2127-422b-91ae-364da26
Cryptology ePrint Archive	af854a3a-2127-422b-91ae-364da26
Security Announcement	af854a3a-2127-422b-91ae-364da26
PGP Corporation - Library - CTO Corner - OpenPGP Flaw	af854a3a-2127-422b-91ae-364da26
US-CERT Vulnerability Note VU#303094	af854a3a-2127-422b-91ae-364da26
eprint.iacr.org/2005/033.pdf	af854a3a-2127-422b-91ae-364da26
SecurityTracker.com Archives - OpenPGP CFB Mode Is Subject to Adaptive Chosen-Plaintext Attacks	af854a3a-2127-422b-91ae-364da26
Advisories - Mandriva	af854a3a-2127-422b-91ae-364da26
Gentoo Linux Documentation -- GnuPG: OpenPGP protocol attack	af854a3a-2127-422b-91ae-364da26
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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