



CVE-2005-3256

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

Summary

CVE	CVE-2005-3256
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-18 21:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The key selection dialogue in Enigmail before 0.92.1 can incorrectly select a key with a user ID that does not have additional

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	Enigmail	Enigmail	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	Link
Debian -- Security Information -- DSA-889-1 enigmail			af854a3a-2127-422b-91ae-364da2661108	www.debian.org
USN-211-1: Enigmail vulnerability Ubuntu security notices			af854a3a-2127-422b-91ae-364da2661108	usn.ubuntu.com
Security Announcement			af854a3a-2127-422b-91ae-364da2661108	www.novell.com
CERT Vulnerability Notes Database			af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org
Advisories - Mandriva Linux			af854a3a-2127-422b-91ae-364da2661108	www.mandriva.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			af854a3a-2127-422b-91ae-364da2661108	www.vupen.com
Mozilla Enigmail Incorrect Encryption Key Selection Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
DFN-CERT: Sicherheitsbulletin Schwachstelle in Enigmail			af854a3a-2127-422b-91ae-364da2661108	www.cert.dfn.de
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.				