CVE-2005-0022

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

Summary

CVE	CVE-2005-0022
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	Buffer overflow in the spa_base64_to_bits function in Exim before 4.43, as originally obtained from Samba code, and as ca

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	University Of Cambridge	Exim	4.41	All	All	All

Application	University Of Cambridge	Exim	4.42	All	All	All
Application	University Of Cambridge	Exim	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	Tags
[exim] 2 smallish security issues	af854a3a-2127-422b-91ae-364da2661108	www.exim.org	Patch
'exim auth_spa_server() PoC exploit' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
Accenture | Let there be change	af854a3a-2127-422b-91ae-364da2661108	www.idefense.com	
Exim SPA Authentication Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org	
Gentoo Linux Documentation -- Exim: Two buffer overflows	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.org	Vend
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com	Patch
404 Not Found	af854a3a-2127-422b-91ae-364da2661108	ftp6.us.freebsd.org	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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