CVE-2008-2575

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

Summary

CVE	CVE-2008-2575
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-06 22:32:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	cbrPager before 0.9.17 allows user-assisted remote attackers to execute arbitrary commands via shell metacharacters in a

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-78 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	7	All	All	All

Operating System	Fedoraproject	Fedora	8	All	All	All
Operating System	Fedoraproject	Fedora	9	All	All	All
Application	Jcoppens	Cbrpager	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
cbrPager download | SourceForge.net	af854a3a-2127-42
Bug 448285 – CVE-2008-2575 cbrpager: Command executions via improper shell escaping	af854a3a-2127-42
cbrPager Archive Handling Arbitrary Command Execution - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-42
Fedora update for cbrpager - Advisories - Secunia	af854a3a-2127-42
Webmail - OVH	af854a3a-2127-42
Gentoo update for cbrpager - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-42
IBM X-Force Exchange	af854a3a-2127-42
cbrPager Change log	af854a3a-2127-42
cvs.fedoraproject.org/viewcvs/rpms/cbrpager/devel/cbrpager-0.9.16-filen-shell-escap...	af854a3a-2127-42
SourceForge.net: News: cbrpager-0.9.17 released	af854a3a-2127-42
cbrPager: User-assisted execution of arbitrary code — Gentoo Linux Documentation	af854a3a-2127-42
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.