CVE-2006-2085

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

Summary

CVE	CVE-2006-2085
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-04-29 10:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple buffer overflows in (1) CxAce60.dll and (2) CxAce60u.dll in SpeedProject Squeez 5.10 Build 4460, and SpeedCom

Risk And Classification

Primary CVSS: v2.0 5.1 from nvd@nist.gov

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

EPSS: 0.049770000 probability, percentile 0.897050000 (date 2026-04-20)

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Speedproject	Speedcommander	10.52_build4450	All	All	All
Application	Speedproject	Speedcommander	11.01_build4450	All	All	All
Application	Speedproject	Squeez	5.10_build_4460	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
SpeedProject Products ACE Archive Handling Buffer Overflow - Secunia Research - Secunia	af854a3
SecurityReason - SpeedProject Products ACE Archive HandlingBuffer Overflow	af854a3
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3
Squeez Buffer Overflows in Processing ACE Archives May Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3
SpeedProject	af854a3
SpeedProject Products ACE Archive Handling Buffer Overflow - Advisories - Secunia	af854a3
Multiple SpeedProject Products ACE Archive Filename Handling Buffer Overflow Vulnerability	af854a3
SecurityFocus	af854a3
www.osvdb.org/24990	af854a3
IBM X-Force Exchange	af854a3
SpeedCommander Buffer Overflows in Processing ACE Archives May Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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