



CVE-2011-5006

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-5006
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-12-25 01:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in QQPlayer 3.2.845 allows remote attackers to execute arbitrary code via a crafted PnSize va

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qqplayer	Qqplayer	3.2.845	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
QQ Player 'PnSize' Value Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
About Secunia Research Flexera	af854a3a-2127-422b-91ae-364da2661108	secunia.com
QQPLAYER PICT PnSize Buffer Overflow WIN7 DEP_ASLR BYPASS	af854a3a-2127-422b-91ae-364da2661108	www.exploit-db.com
www.osvdb.org/77266	af854a3a-2127-422b-91ae-364da2661108	www.osvdb.org
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.