



CVE-2010-2009

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

Summary

CVE	CVE-2010-2009
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-05-21 17:30:00 UTC
Updated	2010-05-24 04:00:00 UTC
Description	Stack-based buffer overflow in the media library in BS.Global BS.Player 2.51 build 1022, 2.41 build 1003, and possibly other

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bsplayer	Bs.player	2.41	All	All	All
Application	Bsplayer	Bs.player	2.51	All	All	All
Application	Bsplayer	Bs.player	2.41	All	All	All
Application	Bsplayer	Bs.player	2.51	All	All	All

References

Reference	Source	Lin
Zero Science Lab » BS.Player v2.51 build 1022 (Media Library) Remote Buffer Overflow Vulnerability	MISC	www
Malformed Request	BID	www
BS.Player BSI File Processing Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	sec
Files ≈ Packet Storm	MISC	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)