



# CVE-2010-2004

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

## Summary

<b>CVE</b>	CVE-2010-2004
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-05-20 21:30:00 UTC
<b>Updated</b>	2017-08-17 01:32:00 UTC
<b>Description</b>	Stack-based buffer overflow in BS.Global BS.Player 2.51 Build 1022 Free, and possibly other versions, allows user-assisted

## 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	2.51	-	free	All
Application	Bsplayer	Bs.player	2.51	-	free	All

## References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Hack 4 Career » Fuzzzzing	MISC
BS.Player BSI File Processing Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
BS.Player v2.51 Universal SEH Overflow Exploit	EXPLOIT-DB
IBM X-Force Exchange	XF
BS.Player '.bsl' File Remote Buffer Overflow Vulnerability	BID
www.mertsarica.com/codes/bsplayer_seh_overwrite.py	MISC
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.

© [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](#)**