



# CVE-2009-4251

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

## Summary

<b>CVE</b>	CVE-2009-4251
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-12-10 00:30:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	Stack-based buffer overflow in Jasc Paint Shop Pro 8.10 (aka Corel Paint Shop Pro) allows user-assisted remote attackers

## 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	Corel	Paint Shop Pro	8.10	All	All	All

## Vendor Declared Affected Products

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

## References

Reference	Source
<a href="https://osvdb.org/60592">osvdb.org/60592</a>	af854a3a-2127-422b
Corel Paint Shop Pro PNG File Handling Remote Buffer Overflow Vulnerability	af854a3a-2127-422b
IBM X-Force Exchange	af854a3a-2127-422b
Luigi Auriemma • View topic - Jasc Paint Shop Pro v8 Local Buffer Overflow Exploit (Univer	af854a3a-2127-422b
Jasc Paint Shop Pro PNG Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b
Files ~ Packet Storm	af854a3a-2127-422b
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b
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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)