



CVE-2007-2244

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

Summary

CVE	CVE-2007-2244
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-25 16:19:00 UTC
Updated	2017-10-11 01:32:00 UTC
Description	Multiple buffer overflows in Adobe Photoshop CS2 and CS3, Illustrator CS3, and GoLive 9 allow user-assisted remote attac

Risk And Classification

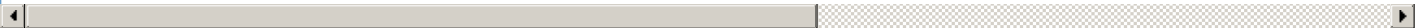
Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Golive	9	All	All	All
Application	Adobe	Golive	9	All	All	All
Application	Adobe	Illustrator	cs3	All	All	All
Application	Adobe	Illustrator	cs3	All	All	All
Application	Adobe	Photoshop	9.0.2	All	All	All
Application	Adobe	Photoshop	9.0.2	All	All	All

References

Reference
38066
Adobe Photoshop Multiple File Format Buffer Overflow Vulnerability
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Adobe Photoshop CS2 / CS3 Unspecified .BMP File Buffer Overflow Exploit
Adobe Illustrator PNG/BMP File Processing Vulnerabilities - Advisories - Secunia
SecurityTracker.com Archives - Adobe Illustrator Input Validation Flaws in Processing BMP, DIB, RLE, or PNG Files Let Remote Users Execu
38064

Adobe Photoshop BMP.8BI Bitmap File Handling Buffer Overflow - Advisories - Secunia
Adobe - Security Advisories : Illustrator CS3 update to address potential security vulnerabilities
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Adobe Photoshop Buffer Overflow in Processing BMP/DIB/RLE Files Lets Remote Users Execute Arbitrary Code - SecurityTracker
IBM X-Force Exchange
Adobe - Security Advisories : Photoshop CS2 and CS3 updates to address security vulnerabilities
35370
38065
Adobe - Security Advisories : GoLive 9 update to address potential security vulnerabilities
Adobe GoLive PNG/BMP File Processing Vulnerabilities - Advisories - Secunia
CVE Program record
NVD vulnerability detail

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](#).

Free CVE JSON API [cve.report/api](#)

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