



# CVE-2007-2365

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

## Summary

|                        |                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2007-2365                                                                                                         |
| <b>State</b>           | PUBLIC                                                                                                                |
| <b>Assigner</b>        | cve@mitre.org                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                          |
| <b>Published</b>       | 2007-04-30 22:19:00 UTC                                                                                               |
| <b>Updated</b>         | 2017-10-11 01:32:00 UTC                                                                                               |
| <b>Description</b>     | Buffer overflow in Adobe Photoshop CS2 and CS3, Photoshop Elements 5.0, Illustrator CS3, and GoLive 9 allows user-ass |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                | Product                            | Version | Update | Edition | Language |
|-------------|-----------------------|------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Adobe</a> | <a href="#">Golive</a>             | 9       | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Golive</a>             | 9       | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Illustrator</a>        | cs3     | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Illustrator</a>        | cs3     | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a>          | 9.0.2   | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a>          | 9.0.2   | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop Elements</a> | 5.0     | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop Elements</a> | 5.0     | All    | All     | All      |

## References

| Reference                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------|
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                         |
| IBM X-Force Exchange                                                                                                                     |
| Adobe Illustrator PNG/BMP File Processing Vulnerabilities - Advisories - Secunia                                                         |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                         |
| SecurityTracker.com Archives - Adobe Illustrator Input Validation Flaws in Processing BMP, DIB, RLE, or PNG Files Let Remote Users Execu |
| Photoshop CS2/CS3 / Paint Shop Pro 11.20 .PNG File BoF Exploit                                                                           |

|                                                                                                    |
|----------------------------------------------------------------------------------------------------|
| Adobe - Security Advisories : Illustrator CS3 update to address potential security vulnerabilities |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                   |
| 38063                                                                                              |
| Adobe Products PNG.8BI PNG File Handling Buffer Overflow - Advisories - Secunia                    |
| 35465                                                                                              |
| Adobe - Security Advisories : Photoshop CS2 and CS3 updates to address security vulnerabilities    |
| Adobe - Security Advisories : GoLive 9 update to address potential security vulnerabilities        |
| Adobe GoLive PNG/BMP File Processing Vulnerabilities - Advisories - Secunia                        |
| Multiple Image Editing Applications .PNG Format Handling Remote Buffer Overflow Vulnerability      |
| CVE Program record                                                                                 |
| NVD vulnerability detail                                                                           |
| <div> <div></div> <div></div> </div>                                                               |
| 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](#)