CVE-2007-2365

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-2365
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-30 22:19:00 UTC
Updated	2017-10-11 01:32:00 UTC
Description	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	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
Application	Adobe	Photoshop Elements	5.0	All	All	All
Application	Adobe	Photoshop Elements	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

No vendor comments have been submitted for this CVE.

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