



CVE-2012-0275

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

Summary

CVE	CVE-2012-0275
State	PUBLISHED
Assigner	flexera
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-04 11:04:48 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Heap-based buffer overflow in Photoshop.exe in Adobe Photoshop CS5 12.x before 12.0.5, CS5.1 12.1.x before 12.1.1, an

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Photoshop Cs5.5	12.0.1	All	All	All

Application	Adobe	Photoshop Cs5.5	12.0.2	All	All	All
Application	Adobe	Photoshop Cs5.5	12.0.3	All	All	All
Application	Adobe	Photoshop Cs5.5	12.0.4	All	All	All
Application	Adobe	Photoshop Cs5.5	12.1	All	All	All
Application	Adobe	Photoshop Cs6	13.0	All	All	All

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

References	
Reference	Source
Adobe Photoshop CVE-2012-0275 Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108
Adobe Photoshop Buffer Overflows Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108
About Secunia Research Flexera	af854a3a-2127-422b-91ae-364da2661108
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108
Adobe - Security Bulletins: APSB12-20 - Security update available for Adobe Photoshop CS6	af854a3a-2127-422b-91ae-364da2661108
Adobe - Security Bulletins: APSB12-11 Security bulletin for Adobe Photoshop	af854a3a-2127-422b-91ae-364da2661108
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.