



# CVE-2012-2028

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

## Summary

|                        |                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-2028                                                                                                           |
| <b>State</b>           | PUBLIC                                                                                                                  |
| <b>Assigner</b>        | psirt@adobe.com                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                            |
| <b>Published</b>       | 2012-05-09 04:36:00 UTC                                                                                                 |
| <b>Updated</b>         | 2017-11-22 02:29:00 UTC                                                                                                 |
| <b>Description</b>     | Buffer overflow in Adobe Photoshop CS5 12.x before 12.0.5 and CS5.1 12.1.x before 12.1.1 allows remote attackers to exe |



## 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="#">Photoshop</a> | All     | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 10.0    | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 10.0.1  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 11.0    | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 11.0    | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 11.0.1  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 11.0.2  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 11.0.4  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 12.0.0  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 12.0.1  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 12.0.2  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 12.0.3  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 12.0.4  | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 2.5     | All    | pro     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 3.0     | All    | pro     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 4.0     | All    | pro     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Photoshop</a> | 5.0     | All    | pro     | All      |

|             |       |           |        |     |     |     |
|-------------|-------|-----------|--------|-----|-----|-----|
|             |       |           |        |     |     |     |
| Application | Adobe | Photoshop | 6.0    | All | All | All |
| Application | Adobe | Photoshop | 6.0    | All | pro | All |
| Application | Adobe | Photoshop | 6.0.1  | All | All | All |
| Application | Adobe | Photoshop | 7.0    | All | All | All |
| Application | Adobe | Photoshop | 7.0.1  | All | All | All |
| Application | Adobe | Photoshop | 8.0    | All | All | All |
| Application | Adobe | Photoshop | 9.0    | All | All | All |
| Application | Adobe | Photoshop | 9.0.1  | All | All | All |
| Application | Adobe | Photoshop | 9.0.2  | All | All | All |
| Application | Adobe | Photoshop | All    | All | All | All |
| Application | Adobe | Photoshop | 10.0   | All | All | All |
| Application | Adobe | Photoshop | 10.0.1 | All | All | All |
| Application | Adobe | Photoshop | 11.0   | All | All | All |
| Application | Adobe | Photoshop | 11.0   | All | All | All |
| Application | Adobe | Photoshop | 11.0.1 | All | All | All |
| Application | Adobe | Photoshop | 11.0.2 | All | All | All |
| Application | Adobe | Photoshop | 11.0.4 | All | All | All |
| Application | Adobe | Photoshop | 12.0.0 | All | All | All |
| Application | Adobe | Photoshop | 12.0.1 | All | All | All |
| Application | Adobe | Photoshop | 12.0.2 | All | All | All |
| Application | Adobe | Photoshop | 12.0.3 | All | All | All |
| Application | Adobe | Photoshop | 12.0.4 | All | All | All |
| Application | Adobe | Photoshop | 2.5    | All | pro | All |
| Application | Adobe | Photoshop | 3.0    | All | pro | All |
| Application | Adobe | Photoshop | 4.0    | All | pro | All |
| Application | Adobe | Photoshop | 5.0    | All | pro | All |
| Application | Adobe | Photoshop | 6.0    | All | All | All |
| Application | Adobe | Photoshop | 6.0    | All | pro | All |
| Application | Adobe | Photoshop | 6.0.1  | All | All | All |
| Application | Adobe | Photoshop | 7.0    | All | All | All |
| Application | Adobe | Photoshop | 7.0.1  | All | All | All |
| Application | Adobe | Photoshop | 8.0    | All | All | All |
| Application | Adobe | Photoshop | 9.0    | All | All | All |
| Application | Adobe | Photoshop | 9.0.1  | All | All | All |
| Application | Adobe | Photoshop | 9.0.2  | All | All | All |

|             |       |                 |      |     |     |     |
|-------------|-------|-----------------|------|-----|-----|-----|
| Application | Adobe | Photoshop Cs4   | 11.0 | All | All | All |
| Application | Adobe | Photoshop Cs4   | 11.0 | All | All | All |
| Application | Adobe | Photoshop Cs5.5 | All  | All | All | All |

| References                                                                                 |  |  |  |          |                                                                                |  |
|--------------------------------------------------------------------------------------------|--|--|--|----------|--------------------------------------------------------------------------------|--|
| Reference                                                                                  |  |  |  | Source   | Link                                                                           |  |
| IBM X-Force Exchange                                                                       |  |  |  | XF       | <a href="https://exchange.xforce.ibmcloud.com/">exchange.xforce.ibmcloud.c</a> |  |
| Adobe Photoshop Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker |  |  |  | SECTrack | <a href="https://www.securitytracker.com">www.securitytracker.com</a>          |  |
| Adobe - Security Bulletins: APSB12-11 Security bulletin for Adobe Photoshop                |  |  |  | CONFIRM  | <a href="https://www.adobe.com">www.adobe.com</a>                              |  |
| Adobe Photoshop CVE-2012-2028 Remote Buffer Overflow Vulnerability                         |  |  |  | BID      | <a href="https://www.securityfocus.com">www.securityfocus.com</a>              |  |
| CVE Program record                                                                         |  |  |  | CVE.ORG  | <a href="https://www.cve.org">www.cve.org</a>                                  |  |
| NVD vulnerability detail                                                                   |  |  |  | NVD      | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                                |  |

No vendor comments have been submitted for this CVE.

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