



# CVE-2015-6710

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

## Summary

|                        |                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-6710                                                                                                       |
| <b>State</b>           | PUBLISHED                                                                                                           |
| <b>Assigner</b>        | adobe                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                        |
| <b>Published</b>       | 2015-10-14 23:59:32 UTC                                                                                             |
| <b>Updated</b>         | 2026-05-06 22:30:45 UTC                                                                                             |
| <b>Description</b>     | The CBBBRInit method in Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat R |

## Risk And Classification

**Primary CVSS:** v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

**Problem Types:** NVD-CWE-noinfo | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Adobe  | Acrobat | All     | All    | All     | All      |

|                  |                           |                                   |     |     |     |     |
|------------------|---------------------------|-----------------------------------|-----|-----|-----|-----|
| Application      | <a href="#">Adobe</a>     | <a href="#">Acrobat</a>           | All | All | All | All |
| Application      | <a href="#">Adobe</a>     | <a href="#">Acrobat Dc</a>        | All | All | All | All |
| Application      | <a href="#">Adobe</a>     | <a href="#">Acrobat Dc</a>        | All | All | All | All |
| Application      | <a href="#">Adobe</a>     | <a href="#">Acrobat Reader</a>    | All | All | All | All |
| Application      | <a href="#">Adobe</a>     | <a href="#">Acrobat Reader</a>    | All | All | All | All |
| Application      | <a href="#">Adobe</a>     | <a href="#">Acrobat Reader Dc</a> | All | All | All | All |
| Application      | <a href="#">Adobe</a>     | <a href="#">Acrobat Reader Dc</a> | All | All | All | All |
| Operating System | <a href="#">Apple</a>     | <a href="#">Macos</a>             | -   | All | All | All |
| Operating System | <a href="#">Microsoft</a> | <a href="#">Windows</a>           | -   | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |
|-----------------------------------|--------------------|---------------------|--------------|---------------|
| Source                            | Vendor             | Product             | Version      | Platforms     |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

| References                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                                                                                                                           |
| Adobe Acrobat/Reader Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Execute Arbitrary Code, and Bypass Security |
| ZDI-15-487   Zero Day Initiative                                                                                                           |
| Adobe Security Bulletin                                                                                                                    |
| 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.