



# CVE-2015-6581

Published on: 09/03/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

## CVE-2015-6581

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

Double free vulnerability in the `opj_j2k_copy_default_tcp_and_create_tcd` function in `j2k.c` in OpenJPEG before r3002, as used in PDFium in Google Chrome before 45.0.2454.85, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering a memory-allocation failure.

CVE-2015-6581 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                                                                                      | Tags                                                                                                                                       | Link                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Issue 526825 - chromium - Tracking bug for internal fixes: Chrome M45, release 0 - An open-source project to help move the web forward. - Google Project Hosting | <a href="#">code.google.com</a><br><a href="#">text/html</a>                                                                               | <b>CONFIRM</b><br><a href="#">code.google.com/p/chromium/issues/detail?id=526825</a>                   |
| Google Code Archive - Long-term storage for Google Code Project Hosting.                                                                                         | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br><b>Inactive Link</b> <b>Not Archived</b>                                   | <b>CONFIRM</b><br><a href="#">code.google.com/p/openjpeg/issues/detail?id=492</a>                      |
| Chrome Releases: Stable Channel Update                                                                                                                           | <a href="#">Patch</a><br><a href="#">Vendor Advisory</a><br><a href="#">googlechromereleases.blogspot.com</a><br><a href="#">text/html</a> | <b>CONFIRM</b><br><a href="#">googlechromereleases.blogspot.com/2015/09/stable-channel-update.html</a> |

|                                                                                                                                                                                  |                                                                                             |                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, Obtain Potentially Sensitive Information, and Spoof Content - SecurityTracker | <a href="http://www.securitytracker.com/text/html">www.securitytracker.com</a><br>text/html | <a href="#">SECTRACK 1033472</a>                                                                                                                                                                              |
| [SECURITY] Fedora 21 Update: openjpeg2-2.1.0-7.fc21                                                                                                                              | <a href="http://lists.fedoraproject.org/text/html">lists.fedoraproject.org</a><br>text/html | <a href="#">FEDORA FEDORA-2015-1c9ed24c61</a>                                                                                                                                                                 |
| [SECURITY] Fedora 22 Update: openjpeg2-2.1.0-7.fc22                                                                                                                              | <a href="http://lists.fedoraproject.org/text/html">lists.fedoraproject.org</a><br>text/html | <a href="#">FEDORA FEDORA-2015-773ef285ef</a>                                                                                                                                                                 |
| Debian -- Security Information -- DSA-3665-1 openjpeg2                                                                                                                           | <a href="http://www.debian.org">www.debian.org</a><br><b>Deprecated Link</b><br>text/html   | <a href="#">DEBIAN DSA-3665</a>                                                                                                                                                                               |
| 486538 - chromium - An open-source project to help move the web forward. - Monorail                                                                                              | <a href="http://code.google.com/text/html">code.google.com</a><br>text/html                 | <a href="http://code.google.com/p/chromium/issues/detail?id=486538">CONFIRM</a><br><a href="http://code.google.com/p/chromium/issues/detail?id=486538">code.google.com/p/chromium/issues/detail?id=486538</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type                           | Vendor                 | Product                | Version | Update | Edition | Language |
|--------------------------------|------------------------|------------------------|---------|--------|---------|----------|
| Application                    | <a href="#">Google</a> | <a href="#">Chrome</a> | All     | All    | All     | All      |
| cpe:2.3:a:google:chrome:*****: |                        |                        |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)