



# CVE-2015-1281

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

## Summary

|                        |                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-1281                                                                                                          |
| <b>State</b>           | PUBLIC                                                                                                                 |
| <b>Assigner</b>        | security@google.com                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                           |
| <b>Published</b>       | 2015-07-23 00:59:00 UTC                                                                                                |
| <b>Updated</b>         | 2023-11-07 02:24:00 UTC                                                                                                |
| <b>Description</b>     | core/loader/ImageLoader.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly determine the V8 |

## Risk And Classification

### Problem Types: CWE-254

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                   | Product                                                    | Version | Update | Edition | Language |
|------------------|--------------------------|------------------------------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>   | <a href="#">Debian Linux</a>                               | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>   | <a href="#">Debian Linux</a>                               | 8.0     | All    | All     | All      |
| Application      | <a href="#">Google</a>   | <a href="#">Chrome</a>                                     | All     | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                   | 13.1    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                   | 13.2    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                   | 13.1    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                   | 13.2    | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Desktop Supplementary</a>     | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Desktop Supplementary</a>     | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Server Supplementary</a>      | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Server Supplementary</a>      | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Server Supplementary Eus</a>  | 6.7z    | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Server Supplementary Eus</a>  | 6.7z    | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Workstation Supplementary</a> | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>   | <a href="#">Enterprise Linux Workstation Supplementary</a> | 6.0     | All    | All     | All      |

## References

| Reference                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------|
| Chromium: Multiple vulnerabilities (GLSA 201603-09) — Gentoo security                                                                          |
| Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information |
| Debian -- Security Information -- DSA-3315-1 chromium-browser                                                                                  |
| Red Hat Customer Portal                                                                                                                        |
| Issue 487155 - chromium - Security: CSP does not block svg image in nested iframe - An open-source project to help move the web forward.       |
| Chrome Releases: Stable Channel Update                                                                                                         |
| Google Chrome Prior to 44.0.2403.89 Multiple Security Vulnerabilities                                                                          |
| [security-announce] openSUSE-SU-2015:1287-1: important: Security update                                                                        |
| [blink] Revision 196071                                                                                                                        |
| CVE Program record                                                                                                                             |
| NVD vulnerability detail                                                                                                                       |
| <div> <div></div> <div></div> </div>                                                                                                           |
| No vendor comments have been submitted for this CVE.                                                                                           |
| There are currently no legacy QID mappings associated with this CVE.                                                                           |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)