

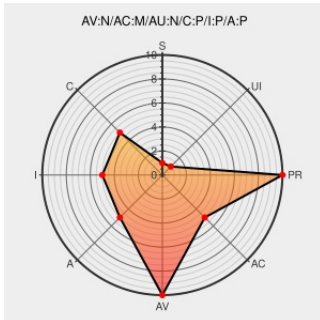


# CVE-2015-4491

Published on: 08/15/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

## CVE-2015-4491

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Integer overflow in the `make_filter_table` function in `pixops/pixops.c` in `gdk-pixbuf` before 2.31.5, as used in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 on Linux, Google Chrome on Linux, and other products, allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and application crash) via crafted bitmap dimensions that are mishandled during scaling.

CVE-2015-4491 has been assigned by [m](#) security@mozilla.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**MEDIUM**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**PARTIAL**

Availability  
Impact

**PARTIAL**

## CVE References

Description

Tags

Link

Oracle Solaris Bulletin - April 2016

[Third Party Advisory](#)  
[www.oracle.com](#)  
[text/html](#)

[CONFIRM](#)  
[www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html](#)

Bug 752297 – heap overflow and DoS affecting Firefox and other programs (x86\_64)

[Issue Tracking](#)  
[bugzilla.gnome.org](#)  
[text/html](#)

[CONFIRM](#) [bugzilla.gnome.org/show\\_bug.cgi?id=752297](#)

[SECURITY] Fedora 22 Update: gdk-pixbuf2-2.31.6-1.fc22

[lists.fedoraproject.org](#)  
[text/html](#)

[FEDORA](#) [FEDORA-2015-13925](#)

[security-announce] openSUSE-SU-2015:1390-1: important: Security update

[Third Party Advisory](#)  
[lists.opensuse.org](#)  
[text/html](#)

[SUSE](#) [openSUSE-SU-2015:1390](#)

|                                                                                                                                                                                                            |                                                                                                           |                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restrictions, and Conduct Cross-Site Scripting Attacks - SecurityTracker | <a href="http://www.securitytracker.com">www.securitytracker.com</a><br>text/html                         |  SECTrack 1033247                                                                                                                                                                |
| Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security                                                                                                                              | <a href="http://security.gentoo.org">security.gentoo.org</a><br>text/html                                 |  GENTOO GLSA-201605-06                                                                                                                                                           |
| gdk-pixbuf: Multiple Vulnerabilities (GLSA 201512-05) — Gentoo Security                                                                                                                                    | <a href="http://security.gentoo.org">security.gentoo.org</a><br>text/html                                 |  GENTOO GLSA-201512-05                                                                                                                                                           |
| Red Hat Customer Portal                                                                                                                                                                                    | <a href="http://web.archive.org">web.archive.org</a><br>text/html<br>Inactive Link Not Archived           |  REDHAT RHSA-2015:1586                                                                                                                                                           |
| Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges - SecurityTracker                                                                      | <a href="http://www.securitytracker.com">www.securitytracker.com</a><br>text/html                         |  SECTrack 1033372                                                                                                                                                                |
| USN-2702-2: Ubufox update   Ubuntu                                                                                                                                                                         | Third Party Advisory<br><a href="http://www.ubuntu.com">www.ubuntu.com</a><br>text/html                   |  UBUNTU USN-2702-2                                                                                                                                                               |
| USN-2722-1: GDK-PixBuf vulnerability   Ubuntu                                                                                                                                                              | <a href="http://www.ubuntu.com">www.ubuntu.com</a><br>text/html                                           |  UBUNTU USN-2722-1                                                                                                                                                               |
| Oracle Solaris Third Party Bulletin - October 2015                                                                                                                                                         | Third Party Advisory<br><a href="http://www.oracle.com">www.oracle.com</a><br>text/html                   |  CONFIRM<br><a href="http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html">www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html</a> |
| USN-2712-1: Thunderbird vulnerabilities   Ubuntu                                                                                                                                                           | <a href="http://www.ubuntu.com">www.ubuntu.com</a><br>text/html                                           |  UBUNTU USN-2712-1                                                                                                                                                             |
| [SECURITY] Fedora 21 Update: mingw-gdk-pixbuf-2.31.6-1.fc21                                                                                                                                                | Third Party Advisory<br><a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a><br>text/html |  FEDORA FEDORA-2015-14010                                                                                                                                                      |
| Access Denied                                                                                                                                                                                              | Issue Tracking<br><a href="http://bugzilla.mozilla.org">bugzilla.mozilla.org</a><br>text/html             |  CONFIRM <a href="http://bugzilla.mozilla.org/show_bug.cgi?id=1184009">bugzilla.mozilla.org/show_bug.cgi?id=1184009</a>                                                        |
| [security-announce] SUSE-SU-2015:1528-1: important: Security update for                                                                                                                                    | <a href="http://lists.opensuse.org">lists.opensuse.org</a><br>text/html                                   |  SUSE SUSE-SU-2015:1528                                                                                                                                                        |
| openSUSE-SU-2015:1453-1: moderate: Security update for MozillaThunderbir                                                                                                                                   | <a href="http://lists.opensuse.org">lists.opensuse.org</a><br>text/html                                   |  SUSE openSUSE-SU-2015:1453                                                                                                                                                    |
| USN-2702-1: Firefox vulnerabilities   Ubuntu                                                                                                                                                               | Third Party Advisory<br><a href="http://www.ubuntu.com">www.ubuntu.com</a><br>text/html                   |  UBUNTU USN-2702-1                                                                                                                                                             |
| USN-2702-3: Firefox regression   Ubuntu                                                                                                                                                                    | <a href="http://www.ubuntu.com">www.ubuntu.com</a><br>text/html                                           |  UBUNTU USN-2702-3                                                                                                                                                             |
| [security-announce] SUSE-SU-2015:1449-1: important: Security update for                                                                                                                                    | <a href="http://lists.opensuse.org">lists.opensuse.org</a><br>text/html                                   |  SUSE SUSE-SU-2015:1449                                                                                                                                                        |
| Red Hat Customer Portal                                                                                                                                                                                    | <a href="http://web.archive.org">web.archive.org</a><br>text/html<br>Inactive Link Not Archived           |  REDHAT RHSA-2015:1694                                                                                                                                                         |
| Debian -- Security Information -- DSA-3337-1 gdk-pixbuf                                                                                                                                                    | <a href="http://www.debian.org">www.debian.org</a><br>Deprecated Link<br>text/html                        |  DEBIAN DSA-3337                                                                                                                                                               |
| [security-announce] openSUSE-SU-2015:1389-                                                                                                                                                                 | Third Party Advisory                                                                                      |  SUSE openSUSE-SU-2015:1389                                                                                                                                                    |

|                                                                                                            |                                                                                                                                  |                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1: important: Security update                                                                              | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br>text/html                                                         |                                                                                                                                                                                                                                                    |
| [SECURITY] Fedora 21 Update: gdk-pixbuf2-2.31.6-1.fc21                                                     | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a><br>text/html                                               |  <a href="#">FEDORA FEDORA-2015-13926</a>                                                                                                                         |
| openSUSE-SU-2015:1500-1: moderate: Security update for gdk-pixbuf                                          | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br>text/html                                                         |  <a href="#">SUSE openSUSE-SU-2015:1500</a>                                                                                                                       |
| Heap overflow in gdk-pixbuf when scaling bitmap images — Mozilla                                           | <a href="#">Vendor Advisory</a><br><a href="https://www.mozilla.org">www.mozilla.org</a><br>text/html                            |  <a href="#">CONFIRM</a><br><a href="https://www.mozilla.org/security/announce/2015/mfsa2015-88.html">www.mozilla.org/security/announce/2015/mfsa2015-88.html</a> |
| openSUSE-SU-2015:1454-1: moderate: Security update for MozillaThunderbir                                   | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br>text/html                                                         |  <a href="#">SUSE openSUSE-SU-2015:1454</a>                                                                                                                       |
| [SECURITY] Fedora 22 Update: mingw-gdk-pixbuf-2.31.6-1.fc22                                                | <a href="#">Third Party Advisory</a><br><a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a><br>text/html       |  <a href="#">FEDORA FEDORA-2015-14011</a>                                                                                                                         |
| [security-announce] SUSE-SU-2015:2081-1: important: Security update for                                    | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br>text/html                                                         |  <a href="#">SUSE SUSE-SU-2015:2081</a>                                                                                                                           |
| Red Hat Customer Portal                                                                                    | <a href="https://web.archive.org">web.archive.org</a><br>text/html<br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  <a href="#">REDHAT RHSA-2015:1682</a>                                                                                                                            |
| Bug 1252290 – CVE-2015-4491 Mozilla: Heap overflow in gdk-pixbuf when scaling bitmap images (MFSa 2015-88) | <a href="#">Issue Tracking</a><br><a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a><br>text/html                     |  <a href="#">CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1252290</a>                                                                                              |
| pixops: Be more careful about integer overflow (ffec86ed) · Commits · GNOME / gdk-pixbuf · GitLab          | <a href="https://git.gnome.org">git.gnome.org</a><br>text/html                                                                   |  <a href="#">CONFIRM git.gnome.org/browse/gdk-pixbuf/commit/?id=ffec86ed5010c5a2be14f47b33bcf4ed3169a199</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 |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 15.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 15.04   | All    | All     | All      |

|                                                       |               |              |        |     |     |     |
|-------------------------------------------------------|---------------|--------------|--------|-----|-----|-----|
| Operating System                                      | Fedoraproject | Fedora       | 21     | All | All | All |
| Operating System                                      | Fedoraproject | Fedora       | 22     | All | All | All |
| Operating System                                      | Fedoraproject | Fedora       | 21     | All | All | All |
| Operating System                                      | Fedoraproject | Fedora       | 22     | All | All | All |
| Application                                           | Gnome         | Gdk-pixbuf   | All    | All | All | All |
| Application                                           | Google        | Chrome       | -      | All | All | All |
| Application                                           | Google        | Chrome       | -      | All | All | All |
| Operating System                                      | Linux         | Linux Kernel | All    | All | All | All |
| Operating System                                      | Linux         | Linux Kernel | All    | All | All | All |
| Application                                           | Mozilla       | Firefox      | All    | All | All | All |
| Application                                           | Mozilla       | Firefox      | All    | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.0   | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.0.1 | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.0.5 | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.1.0 | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.0   | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.0.1 | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.0.5 | All | All | All |
| Application                                           | Mozilla       | Firefox Esr  | 38.1.0 | All | All | All |
| Operating System                                      | Opensuse      | Opensuse     | 13.1   | All | All | All |
| Operating System                                      | Opensuse      | Opensuse     | 13.2   | All | All | All |
| Operating System                                      | Opensuse      | Opensuse     | 13.1   | All | All | All |
| Operating System                                      | Opensuse      | Opensuse     | 13.2   | All | All | All |
| Operating System                                      | Oracle        | Solaris      | 10     | All | All | All |
| Operating System                                      | Oracle        | Solaris      | 11.3   | All | All | All |
| Operating System                                      | Oracle        | Solaris      | 10     | All | All | All |
| Operating System                                      | Oracle        | Solaris      | 11.3   | All | All | All |
| cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*: |               |              |        |     |     |     |

|                                                       |
|-------------------------------------------------------|
| cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*: |
| cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:     |
| cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*: |
| cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*: |
| cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:     |
| cpe:2.3:o:fedoraproject:fedora:21:*:*:*:*:*:          |
| cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:          |
| cpe:2.3:o:fedoraproject:fedora:21:*:*:*:*:*:          |
| cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:          |
| cpe:2.3:a:gnome:gdk-pixbuf:*:*:*:*:*:                 |
| cpe:2.3:a:google:chrome:-:*:*:*:*:*:                  |
| cpe:2.3:a:google:chrome:-:*:*:*:*:*:                  |
| cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:               |
| cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:               |
| cpe:2.3:a:mozilla:firefox:*:*:*:*:*:                  |
| cpe:2.3:a:mozilla:firefox:*:*:*:*:*:                  |
| cpe:2.3:a:mozilla:firefox_esr:38.0:*:*:*:*:*:         |
| cpe:2.3:a:mozilla:firefox_esr:38.0.1:*:*:*:*:*:       |
| cpe:2.3:a:mozilla:firefox_esr:38.0.5:*:*:*:*:*:       |
| cpe:2.3:a:mozilla:firefox_esr:38.1.0:*:*:*:*:*:       |
| cpe:2.3:a:mozilla:firefox_esr:38.0:*:*:*:*:*:         |
| cpe:2.3:a:mozilla:firefox_esr:38.0.1:*:*:*:*:*:       |
| cpe:2.3:a:mozilla:firefox_esr:38.0.5:*:*:*:*:*:       |
| cpe:2.3:a:mozilla:firefox_esr:38.1.0:*:*:*:*:*:       |
| cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:           |
| cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:           |
| cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:           |
| cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:           |

|                                          |
|------------------------------------------|
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |

|                                          |
|------------------------------------------|
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |

|                                          |
|------------------------------------------|
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |

|                                          |
|------------------------------------------|
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |
| cpe:2.3:o:oracle:solaris:10:*:*:*:*:*:   |
| cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)