



CVE-2013-0800

Published on: 04/03/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:41 PM UTC

CVE-2013-0800

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

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

Integer signedness error in the `pixman_fill_sse2` function in `pixman-sse2.c` in `Pixman`, as distributed with `Cairo` and used in `Mozilla Firefox` before 20.0, `Firefox ESR` 17.x before 17.0.5, `Thunderbird` before 17.0.5, `Thunderbird ESR` 17.x before 17.0.5, `SeaMonkey` before 2.17, and other products, allows remote attackers to execute arbitrary code

via crafted values that trigger attempted use of a (1) negative box boundary or (2) negative box size, leading to an out-of-bounds write operation.

CVE-2013-0800 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

Debian -- Security Information -- DSA-2699-1 iceweasel

[Third Party Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-2699](#)

Repository / Oval Repository

[Third Party Advisory](#)
[oval.cisecurity.org](#)
[text/html](#)

[OVAL oval:org.mitre.oval:def:16909](#)

Red Hat Customer Portal

[Broken Link](#)
[web.archive.org](#)
[text/html](#)

[REDHAT RHSA-2013:0696](#)

Inactive Link Not Archived

MFSA 2013-31: Out-of-bounds write in Cairo library

Vendor Advisory
www.mozilla.org
text/html

 CONFIRM
www.mozilla.org/security/announce/2013/mfsa2013-31.html

[security-announce] SUSE-SU-2013:0645-1: important: Security update for

Mailing List
Third Party Advisory
lists.opensuse.org
text/html

 SUSE SUSE-SU-2013:0645

Red Hat Customer Portal

Broken Link
web.archive.org
text/html
Inactive Link Not Archived

 REDHAT RHSA-2013:0697

[security-announce] SUSE-SU-2013:0850-1: important: Security update for

Mailing List
Third Party Advisory
lists.opensuse.org
text/html

 SUSE SUSE-SU-2013:0850

openSUSE-SU-2013:0875-1: moderate: seamonkey: 2.17 update

Mailing List
Third Party Advisory
lists.opensuse.org
text/html

 SUSE openSUSE-SU-2013:0875

[security-announce] openSUSE-SU-2013:0630-1: important: Mozilla Firefox

Mailing List
Third Party Advisory
lists.opensuse.org
text/html

 SUSE openSUSE-SU-2013:0630

USN-1791-1: Thunderbird vulnerabilities | Ubuntu

Third Party Advisory
www.ubuntu.com
text/html

 UBUNTU USN-1791-1

825721 – (CVE-2013-0800) OOB Write in pixman_fill_sse2

Issue Tracking
Patch
Vendor Advisory
bugzilla.mozilla.org
text/html

 CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=825721

[security-announce] openSUSE-SU-2013:0631-1: important: Mozilla Firefox

Mailing List
Third Party Advisory
lists.opensuse.org
text/html

 SUSE openSUSE-SU-2013:0631

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All

System	Category	Product	Version	Architecture	Platform	OS
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Application	Mozilla	Thunderbird Esr	All	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All

Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All
cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:-:*:*:						

cpe:2.3:o:canonical:ubuntu_linux:12.10:****:*:*:
cpe:2.3:o:debian:debian_linux:7.0:****:*:*:
cpe:2.3:o:debian:debian_linux:7.0:****:*:*:
cpe:2.3:a:mozilla:firefox:****:*:*:
cpe:2.3:a:mozilla:firefox:****:*:*:
cpe:2.3:a:mozilla:firefox_esr:****:*:*:
cpe:2.3:a:mozilla:firefox_esr:****:*:*:
cpe:2.3:a:mozilla:seamonkey:****:*:*:
cpe:2.3:a:mozilla:seamonkey:****:*:*:
cpe:2.3:a:mozilla:thunderbird:****:*:*:
cpe:2.3:a:mozilla:thunderbird:****:*:*:
cpe:2.3:a:mozilla:thunderbird_esr:****:*:*:
cpe:2.3:a:mozilla:thunderbird_esr:****:*:*:
cpe:2.3:o:opensuse:opensuse:11.4:****:*:*:
cpe:2.3:o:opensuse:opensuse:12.1:****:*:*:
cpe:2.3:o:opensuse:opensuse:12.2:****:*:*:
cpe:2.3:o:opensuse:opensuse:12.3:****:*:*:
cpe:2.3:o:opensuse:opensuse:11.4:****:*:*:
cpe:2.3:o:opensuse:opensuse:12.1:****:*:*:
cpe:2.3:o:opensuse:opensuse:12.2:****:*:*:
cpe:2.3:o:opensuse:opensuse:12.3:****:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp4:*:*:-*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:-*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp4:*:*:-*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:-*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp4:*:*:-*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:ltss:-*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:ltss:vmware:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:-*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:vmware:*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp4:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:ltss:-:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:ltss:vmware:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:vmware:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp4:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:11:sp2:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp4:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:11:sp2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)