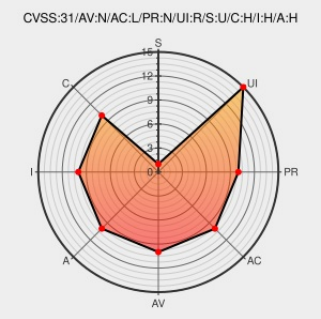
CVE-2010-1772

Published on: 09/24/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:04 PM UTC

CVE-2010-1772

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Use-after-free vulnerability in page/Geolocation.cpp in WebCore in WebKit before r59859, as used in Google Chrome before 5.0.375.70, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted web site, related to failure to stop timers associated with geolocation upon deletion of a document.

CVE-2010-1772 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11661

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Broken Link www.vupen.com text/html	VUPEN ADV-2011-0212
Issue 44868 - chromium - Geolocation events fire after document deletion - Project Hosting on Google Code	Exploit Issue Tracking Mailing List Vendor Advisory code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=44868
596498 – (CVE-2010-1772) CVE-2010-1772 WebKit: use-after-free vulnerability in handling of geolocation events	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=596498
Changeset 59859 – WebKit	Mailing List Patch Vendor Advisory trac.webkit.org text/html	CONFIRM trac.webkit.org/changeset/59859
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Broken Link www.vupen.com text/html	VUPEN ADV-2010-2722
[SECURITY] Fedora 12 Update: qt-4.6.3-8.fc12	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2010-11020
Ubuntu update for webkit - Secunia.com	Broken Link web.archive.org text/html	SECUNIA 41856
[SECURITY] Fedora 13 Update: qt-4.6.3-8.fc13	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2010-11011
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Broken Link www.vupen.com text/html	VUPEN ADV-2011-0552
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Broken Link www.vupen.com text/html	VUPEN ADV-2010-1801
USN-1006-1: WebKit vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-1006-1
Access Denied	Permissions Required Vendor Advisory bugs.webkit.org text/html	CONFIRM bugs.webkit.org/show_bug.cgi?id=39388
Fedora update for qt - Advisories - Community	Broken Link web.archive.org text/html	SECUNIA 40557
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:002	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SR:2011:002

Google Chrome Releases: Stable Channel Update	Release Notes Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2010/06/stable-channel-update.html
Google Chrome Multiple Vulnerabilities - Advisories - Community	Broken Link web.archive.org text/html	SECUNIA 40072
Support / Security / Advisories / / MDVSA-2011:039 | Mandriva	Broken Link www.mandriva.com text/html	MANDRIVA MDVSA-2011:039
SUSE update for Multiple Packages - Secunia.com	Broken Link web.archive.org text/html	SECUNIA 43068

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	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All

Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:12:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:13:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:12:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:13:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report