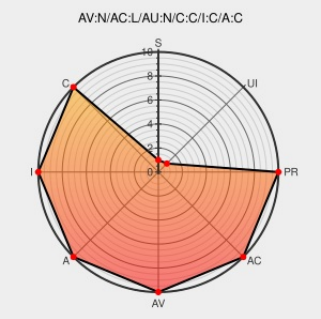
CVE-2010-2302

Published on: 06/15/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:09 PM UTC

CVE-2010-2302

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



Certain versions of Chrome from Google contain the following vulnerability:

Use-after-free vulnerability in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via vectors involving remote fonts in conjunction with shadow DOM trees, aka rdar problem 8007953. NOTE: this might overlap CVE-2010-1771.

CVE-2010-2302 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Permissions Required www.vupen.com text/html	VUPEN ADV-2011-0212
Issue 44740 - chromium - Need to merge fix for WebKit font issue to 375 branch - Project Hosting on Google Code	Vendor Advisory code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=44740
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11948
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:002	Mailing List Third Party Advisory lists.opensuse.org	SUSE SUSE-SR:2011:002

	text/html	
Google Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2010/06/stable-channel-update.html
Google Chrome Multiple Vulnerabilities - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 40072
SUSE update for Multiple Packages - Secunia.com	Third Party Advisory 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
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	Suse	Suse Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All

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:suse:suse_linux_enterprise_desktop:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_desktop:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:10:sp3:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→