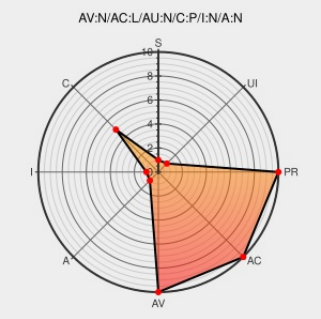
CVE-2013-6630

Published on: 11/15/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

CVE-2013-6630

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



Certain versions of Chrome from Google contain the following vulnerability:

The get_dht function in jdmarker.c in libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48 and other products, does not set all elements of a certain Huffman value array during the reading of segments that follow Define Huffman Table (DHT) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.

CVE-2013-6630 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Oracle Solaris Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098
openSUSE-SU-2014:0008-1: moderate: update for seamonkey	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0008
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1803
MFSA 2013-116:	www.mozilla.org	CONFIRM www.mozilla.org/security/announce/2013/mfsa2013-116.html

JPEG information leak	text/html	
chromium Git repositories - Git at Google	git.chromium.org text/html	CONFIRM git.chromium.org/gitweb/?p=chromium/deps/libjpeg_turbo.git;a=commit;h=32cab49bd4cb1ce069a435fd75f943
openSUSE-SU-2013:1958-1: moderate: update for MozillaThunderbird	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1958
Mageia Advisory: MGASA-2013-0333 - Updated libjpeg packages fix vulnerabilities in libjpeg-turbo	advisories.mageia.org text/html	CONFIRM advisories.mageia.org/MGASA-2013-0333.html
USN-2052-1: Firefox vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2052-1
[SECURITY] Fedora 20 Update: firefox-26.0-3.fc20	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-23519
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1029470
[SECURITY] Fedora 18 Update: thunderbird-24.2.0-2.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-23291
Issue 299835 - chromium - libjpeg_turbo huffval infoleak - An open-source project to help move the web forward. - Google Project Hosting	code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=299835
Security Advisory SA56175 - Ubuntu update for libjpeg and libjpeg-turbo - Secunia	web.archive.org text/html	SECUNIA 56175
Mozilla Seamonkey Multiple Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks -	www.securitytracker.com text/html	SECTRACK 1029476

Scripting Attacks - SecurityTracker		
openSUSE-SU-2014:0065-1: moderate: update for chromium	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0065
openSUSE-SU-2013:1918-1: moderate: update for MozillaFirefox	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1918
USN-2053-1: Thunderbird vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2053-1
[SECURITY] Fedora 19 Update: firefox-26.0-2.fc19	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-23127
[security-announce] openSUSE-SU-2013:1861-1: important: chromium: update	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1861
openSUSE-SU-2013:1917-1: moderate: update for MozillaFirefox	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1917
USN-2060-1: libjpeg, libjpeg-turbo vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2060-1
[security-announce] openSUSE-SU-2013:1776-1: important: chromium: 31.0.1	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1776
Support / Security / Advisories / / MDVSA-2013:273 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:273
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20131112 bugs in IJG jpeg6b & libjpeg-turbo
[security-announce] openSUSE-SU-2013:1777-1: important: chromium: update	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1777
openSUSE-SU-2013:1916-1: moderate: update for MozillaFirefox	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1916

libjpeg-turbo: Multiple vulnerabilities (GLSA 201606-03) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201606-03
Debian -- Security Information -- DSA-2799-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-2799
openSUSE-SU-2013:1957-1: moderate: update for MozillaThunderbird	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1957
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2013/11/stable-channel-update.
891693 – (CVE-2013-6629) JPEG info leak	bugzilla.mozilla.org text/html	CONFIRM bugzilla.mozilla.org/show_bug.cgi?id=891693
[SECURITY] Fedora 19 Update: thunderbird-24.2.0-2.fc19	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-23295
openSUSE-SU-2013:1959-1: moderate: update for MozillaThunderbird	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1959

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	31.0.1650.0	All	All	All
Application	Google	Chrome	31.0.1650.10	All	All	All
Application	Google	Chrome	31.0.1650.11	All	All	All
Application	Google	Chrome	31.0.1650.12	All	All	All
Application	Google	Chrome	31.0.1650.13	All	All	All
Application	Google	Chrome	31.0.1650.14	All	All	All
Application	Google	Chrome	31.0.1650.15	All	All	All
Application	Google	Chrome	31.0.1650.16	All	All	All

Application	Google	Chrome	31.0.1650.17	All	All	All
Application	Google	Chrome	31.0.1650.18	All	All	All
Application	Google	Chrome	31.0.1650.19	All	All	All
Application	Google	Chrome	31.0.1650.2	All	All	All
Application	Google	Chrome	31.0.1650.20	All	All	All
Application	Google	Chrome	31.0.1650.22	All	All	All
Application	Google	Chrome	31.0.1650.23	All	All	All
Application	Google	Chrome	31.0.1650.25	All	All	All
Application	Google	Chrome	31.0.1650.26	All	All	All
Application	Google	Chrome	31.0.1650.27	All	All	All
Application	Google	Chrome	31.0.1650.28	All	All	All
Application	Google	Chrome	31.0.1650.29	All	All	All
Application	Google	Chrome	31.0.1650.3	All	All	All
Application	Google	Chrome	31.0.1650.30	All	All	All
Application	Google	Chrome	31.0.1650.31	All	All	All
Application	Google	Chrome	31.0.1650.32	All	All	All
Application	Google	Chrome	31.0.1650.33	All	All	All
Application	Google	Chrome	31.0.1650.34	All	All	All
Application	Google	Chrome	31.0.1650.35	All	All	All
Application	Google	Chrome	31.0.1650.36	All	All	All
Application	Google	Chrome	31.0.1650.37	All	All	All
Application	Google	Chrome	31.0.1650.38	All	All	All
Application	Google	Chrome	31.0.1650.39	All	All	All
Application	Google	Chrome	31.0.1650.4	All	All	All
Application	Google	Chrome	31.0.1650.41	All	All	All
Application	Google	Chrome	31.0.1650.42	All	All	All
Application	Google	Chrome	31.0.1650.43	All	All	All
Application	Google	Chrome	31.0.1650.44	All	All	All
Application	Google	Chrome	31.0.1650.45	All	All	All
Application	Google	Chrome	31.0.1650.46	All	All	All
Application	Google	Chrome	31.0.1650.5	All	All	All
Application	Google	Chrome	31.0.1650.6	All	All	All
Application	Google	Chrome	31.0.1650.7	All	All	All
Application	Google	Chrome	31.0.1650.8	All	All	All
Application	Google	Chrome	31.0.1650.9	All	All	All

Application	Google	Chrome	31.0.1650.0	All	All	All
Application	Google	Chrome	31.0.1650.10	All	All	All
Application	Google	Chrome	31.0.1650.11	All	All	All
Application	Google	Chrome	31.0.1650.12	All	All	All
Application	Google	Chrome	31.0.1650.13	All	All	All
Application	Google	Chrome	31.0.1650.14	All	All	All
Application	Google	Chrome	31.0.1650.15	All	All	All
Application	Google	Chrome	31.0.1650.16	All	All	All
Application	Google	Chrome	31.0.1650.17	All	All	All
Application	Google	Chrome	31.0.1650.18	All	All	All
Application	Google	Chrome	31.0.1650.19	All	All	All
Application	Google	Chrome	31.0.1650.2	All	All	All
Application	Google	Chrome	31.0.1650.20	All	All	All
Application	Google	Chrome	31.0.1650.22	All	All	All
Application	Google	Chrome	31.0.1650.23	All	All	All
Application	Google	Chrome	31.0.1650.25	All	All	All
Application	Google	Chrome	31.0.1650.26	All	All	All
Application	Google	Chrome	31.0.1650.27	All	All	All
Application	Google	Chrome	31.0.1650.28	All	All	All
Application	Google	Chrome	31.0.1650.29	All	All	All
Application	Google	Chrome	31.0.1650.3	All	All	All
Application	Google	Chrome	31.0.1650.30	All	All	All
Application	Google	Chrome	31.0.1650.31	All	All	All
Application	Google	Chrome	31.0.1650.32	All	All	All
Application	Google	Chrome	31.0.1650.33	All	All	All
Application	Google	Chrome	31.0.1650.34	All	All	All
Application	Google	Chrome	31.0.1650.35	All	All	All
Application	Google	Chrome	31.0.1650.36	All	All	All
Application	Google	Chrome	31.0.1650.37	All	All	All
Application	Google	Chrome	31.0.1650.38	All	All	All
Application	Google	Chrome	31.0.1650.39	All	All	All
Application	Google	Chrome	31.0.1650.4	All	All	All
Application	Google	Chrome	31.0.1650.41	All	All	All
Application	Google	Chrome	31.0.1650.42	All	All	All
Application	Google	Chrome	31.0.1650.43	All	All	All
Application	Google	Chrome	31.0.1650.44	All	All	All

Application	Google	Chrome	31.0.1650.45	All	All	All
Application	Google	Chrome	31.0.1650.46	All	All	All
Application	Google	Chrome	31.0.1650.5	All	All	All
Application	Google	Chrome	31.0.1650.6	All	All	All
Application	Google	Chrome	31.0.1650.7	All	All	All
Application	Google	Chrome	31.0.1650.8	All	All	All
Application	Google	Chrome	31.0.1650.9	All	All	All
Application	Google	Chrome	All	All	All	All

cpe:2.3:a:google:chrome:31.0.1650.0:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.10:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.11:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.12:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.13:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.14:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.15:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.16:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.17:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.18:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.19:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.2:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.20:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.22:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.23:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.25:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.26:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.27:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.28:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.29:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.3:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.30:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.31:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.32:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.33:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.34:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.35:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.36:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.37:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.38:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.39:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.4:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.41:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.42:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.43:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.44:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.45:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.46:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.5:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.6:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.7:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.8:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.9:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.0:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.10:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.11:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.12:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.13:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.14:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.15:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.16:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.17:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.18:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.19:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.2:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.20:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.22:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.23:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.25:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.26:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.27:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.28:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.29:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.3:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.30:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.31:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.32:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.33:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.34:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.35:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.36:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.37:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.38:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.39:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.4:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.41:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.42:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.43:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.44:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.44:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.45:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.46:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.5:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.6:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.7:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.8:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:31.0.1650.9:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→