



CVE-2013-6628

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2013-6628
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-13 15:55:00 UTC
Updated	2017-09-19 01:36:00 UTC
Description	net/socket/ssl_client_socket_nss.cc in the TLS implementation in Google Chrome before 31.0.1650.48 does not ensure tha

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References
Reference
Triple Handshakes Considered Harmful: Breaking and Fixing Authentication over TLS
[chrome] Revision 229611
openSUSE-SU-2014:0065-1: moderate: update for chromium
Repository / Oval Repository
[security-announce] openSUSE-SU-2013:1861-1: important: chromium: update
[security-announce] openSUSE-SU-2013:1776-1: important: chromium: 31.0.1
[security-announce] openSUSE-SU-2013:1777-1: important: chromium: update
Debian -- Security Information -- DSA-2799-1 chromium-browser
Issue 306959 - chromium - Server certificate is not checked during TLS renegotiation - An open-source project to help move the web forward.
Chrome Releases: Stable Channel Update
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.