



CVE-2011-3922

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

Summary

CVE	CVE-2011-3922
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-01-07 11:55:00 UTC
Updated	2023-11-07 02:08:00 UTC
Description	Stack-based buffer overflow in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or p

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All

References

Reference	Source	Link
108006 - chromium - An open-source project to help move the web forward. - Monorail		code.google.com
Chrome Releases: Stable Channel Update	CONFIRM	googlechromereleases.blogspot.c
About Secunia Research Flexera		secunia.com
Google Chrome Multiple Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker		www.securitytracker.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Google Chrome Prior to 16.0.912.75 Multiple Security Vulnerabilities		www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)