



CVE-2011-3066

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

Summary

CVE	CVE-2011-3066
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-04-05 22:02:00 UTC
Updated	2020-04-14 14:59:00 UTC
Description	Skia, as used in Google Chrome before 18.0.1025.151, does not properly perform clipping, which allows remote attackers to

Risk And Classification

Problem Types: CWE-125

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
Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities
Google Chrome Multiple Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker
Issue 106577 - chromium - Heap-buffer-overflow in SkAAClipBlitter::blitAntiH - An open-source project to help move the web forward. - Google
Repository / Oval Repository
Security Alerts - Secunia
Security Advisory SA48749 - Gentoo update for chromium - Secunia
Chrome Releases: Stable and Beta Channel Updates
Google Chrome Prior to 18.0.1025.151 Multiple Security Vulnerabilities
81036
IBM X-Force Exchange
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.

© [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](#)