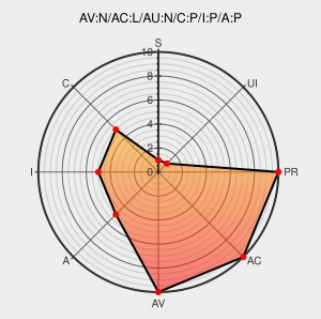
CVE-2011-3925

Published on: 01/23/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:14 PM UTC

CVE-2011-3925

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



Certain versions of Chrome from Google contain the following vulnerability:

Use-after-free vulnerability in the Safe Browsing feature in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors related to a navigation entry and an interstitial page.

CVE-2011-3925 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Repository / Oval Repository	Third Party Advisory, oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:14538
About Secunia Research | Flexera	Third Party Advisory, secunia.com, Depreciated Link, text/plain	SECUNIA 47449
Google Chrome Multiple Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1026487
Chrome Releases: Stable Channel Update	Vendor Advisory, googlechromereleases.blogspot.com, text/html	CONFIRM googlechromereleases.blogspot.com/2012/01/stable-channel-update_23.html

Issue 107182 - chromium - Heap use after free with malware blocking page - An open-source browser project to help move the web forward. - Google Project Hosting	Exploit Issue Tracking Patch Vendor Advisory code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=107182

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→