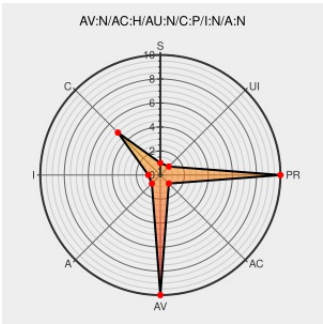
CVE-2012-4930

Published on: 09/15/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:15 PM UTC

CVE-2012-4930

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



Certain versions of Chrome from Google contain the following vulnerability:

The SPDY protocol 3 and earlier, as used in Mozilla Firefox, Google Chrome, and other products, can perform TLS encryption of compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.

CVE-2012-4930 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.6 - LOW

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

CVE References

Description	Tags	Link
Bug 857737 – CVE-2012-4930 SPDY: SSL/TLS CRIME attack	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=857737
The perfect CRIME? New HTTPS web hijack attack explained • The Register	www.theregister.co.uk text/html	MISC www.theregister.co.uk/2012/09/14/crime_tls_attack/
Compression and Information Leakage of Plaintext	www.iacr.org text/html	MISC www.iacr.org/cryptodb/data/paper.php?pubkey=3091
ekoparty Security Conference	web.archive.org text/html Inactive Link Not Archived	MISC www.ekoparty.org/2012/thai-duong.php

Details on the “CRIME” attack - Blog - iSEC Partners	web.archive.org text/html Inactive Link Not Archived	MISC isecpartners.com/blog/2012/9/14/details-on-the-crime-attack.html
CRIME: Information Leakage Attack against SSL/TLS | Qualys Security Labs | Qualys Community	community.qualys.com text/html	MISC community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls
Crack in Internet’s foundation of trust allows HTTPS session hijacking | Ars Technica	arstechnica.com text/html	MISC arstechnica.com/security/2012/09/crime-hijacks-https-sessions/
CRIME Attack Uses Compression Ratio of TLS Requests as Side Channel to Hijack Secure Sessions | threatpost	threatpost.com text/html	MISC threatpost.com/en_us/blogs/crime-attack-uses-compression-ratio-tls-requests-side-channel-hijack-secure-sessions-091312
[security-announce] SUSE-SU-2012:1351-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2012:1351

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
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

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

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

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report