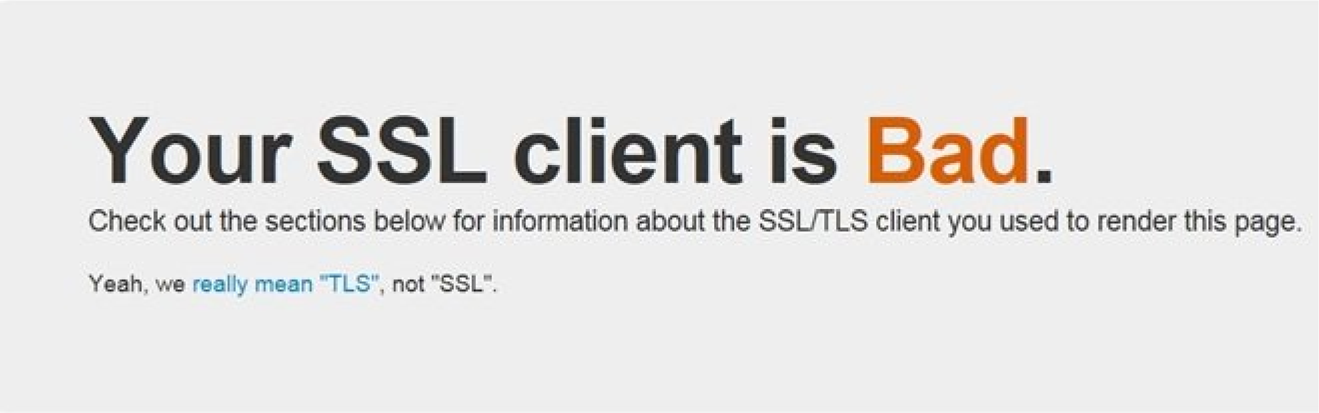
禪

راهنمای عملی قویسازی رمزنگاری در سیستمعامل و مرورگرهای وب



Your SSL client is Bad.

Check out the sections below for information about the SSL/TLS client you used to render this page.

Yeah, we really mean "TLS", not "SSL".

در مقاله "چگونه سازمانهای جاسوسی روزانه به میلیاردها صفحه وب رمزنگاری دسترسی دارند؟ " به نقص امنیتی موجود در الگوریتم رمزنگاری دیفن -هلمن اشاره کردیم و دیدیم آژانسهای جاسوسی بدون اطلاع کاربران از آسیبپذیری موجود در این الگوریتم بهرهبرداری کردند . همچنین دیدیم سایتهایی که به الگوریتم کلید 1024 بیتی رمزنگاری دیفنهلمن اعتماد کرده بودند به آسانی قربانی یک آسیبپذیری امنیتی شدند . بر همین اساس کارشناسان امنیتی توصیه کردند از رمزنگاری 2048 بیتی دیفن هلمن استفاده شود . اکنون در این مقاله قصد داریم راهکارهای ویژهای را به شما معرفی کنیم تا سطح رمزنگاری ارتباطات خود را افزایش داده تا از گزند سرقت اطلاعات دور باشید .

دو کارشناس دنیای امنیت آلکس هالدرمان و نادیا هانینگر در مقاله خود نشان دادند آژانس امنیتی NSA چگونه توانایی رمزگشایی حجم وسیعی از ارتباطات مبتنی بر HTTPS، VPN، SSH را با پیادهسازی یک مکانیزم حمله روی الگوریتم تعویض کلید 1024 بیتی دیفنهلمن دارند . مقاله منتشر شده از سوی این دو کارشناس بازتاب گستردهای در محافل علمی پیدا کرد . البته این دو کارشناس سابقه بررسی الگوریتم رمزنگاری دیفنهلمن را پیش از این نیز داشتند . در اوایل سال جاری میلادی، این گروه تحقیقاتی، حمله Logjam را کالبد شکافی کردند . تجزیه و تحلیل الگوریتم 1024 بیتی دیفن هلمن و مقایسه تکنیک مورد استفاده NSA و در ادامه بررسی مستندات افشا شده، نشان داد این سازمان از مدتها و در اختفای کامل توانایی شکستن کلیدهای 1024 دیفن هلمن را داشته است. اما خبرها همیشه منفی نیست، و خبرهای خوبی نیز وجود دارد . تحقیقات اخیر نشان داده است، تولیدکنندگان بزرگ مرورگرهای اینترنتی (موزیلا، مایکروسافت و گوگل) پشتیبانی از الگوریتم 512 بیتی دیفن هلمن را کنار گذاشتهاند، در نتیجه نگرانی از بابت یکی از بزرگترین آسیبپذیریهای موجود برای همیشه از میان رفت . با این حال، پشتیبانی از کلید 1024 بیت دیفن هلمن همچنان تحت نظارت آژانس NSA قرار داشته و برای کاربردهایی که ممکن است در آینده به آن احتیاج شود، در مرورگرها قرار خواهد گرفت .

مطلب پیشنهادی: چگونه سازمانهای جاسوسی روزانه به میلیاردها صفحه وب رمزنگاری دسترسی دارند؟

در کنار نکات امنیتی که توسط سازندگان مرورگرها لحاظ میشود، ما کاربران مرورگرها میتوانیم یکسری تنظیمات را شخصا مورد بررسی قرار دهیم تا خطر احتمالی را کمی از خود دور کنیم . بر همین اساس در این پست، در نظر داریم، راهکارهایی را به شما معرفی کنیم تا ضریب امنیت مرورگر شما افزایش پیدا کرده و

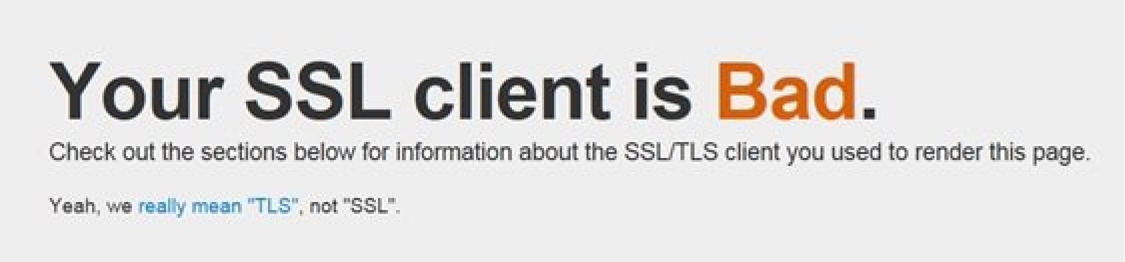
بتوانید از دستگاه، مرورگر کلاینت SSH یا نرمافزار VPN که از آن استفاده میکنید محافظت کنید .

مرورگرهای وب

چگونه میتوانیم اطمینان حاصل کنیم مرورگر ما از الگوریتم رمزنگاری قدرتمندی استفاده میکند؟ جواب ساده است. باید به الگوریتمهای رمزنگاری (یا بستههای سایفری) که مرورگرهای ما از آنها پشتیبانی میکنند نگاهی داشته باشیم . اما روش سادهتری برای این بررسی وجود دارد . How’s My SSL نمونهای از این راهکارها به شمار میرود . این ابزار بسته سایفر مرورگر شما را در ارتباط با پروتکل امنیتی SSL مورد بررسی قرار میدهد . زمانیکه آدرس این سایت را در مرورگر خود وارد کنید، در پایین صفحه توضیحاتی در ارتباط با بستههای سایفر مورد استفاده توسط مرورگر خود را مشاهده میکنید . اگر عبارت _DHE_ را در فهرست رمزها مشاهده نکنید به این معنا است که مرورگر شما در امنیت قرار دارد . هر چند شکلهای مختلفی از رمزنگاری مبتنی بر منحنی بیضوی (Elliptic Curve) وجود دارند، اما اگر عبارت _ECDHE_ را همراه با آنها مشاهده کردید، هیچ جای نگرانی وجود ندارد، به این معنا که در امنیت قرار دارید .

وضعیت مرورگرهای ما چگونه است؟

زمانیکه آدرس How’s My SSL را در مرورگر اینترنت اکسپلورر 11 وارد کردیم، اطلاعات زیر را مشاهده کردیم .

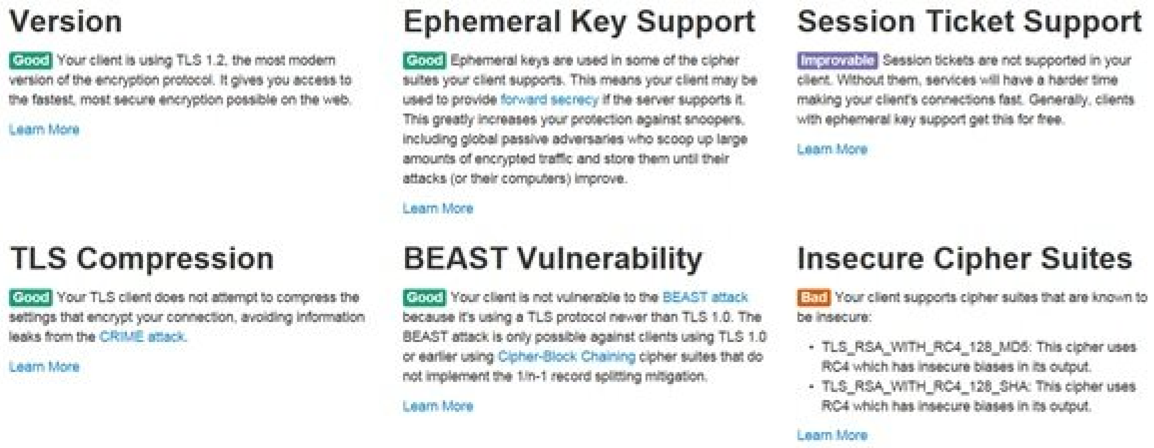


Your SSL client is Bad.

Check out the sections below for information about the SSL/TLS client you used to render this page.

Yeah, we really mean "TLS", not "SSL".

در ادامه وضعیت گزارشی از وضعیت پروتکلهای امنیتی، نسخه مورد استفاده و اطلاعات دیگر را مشاهده کردیم . همانگونه که در تصویر زیر مشاهده میکنید، وضعیت بسته سایفر ما غیرایمن گزارش شده است .



Version

Good Your client is using TLS 1.2, the most modern version of the encryption protocol. It gives you access to the fastest, most secure encryption possible on the web.

Learn More

Ephemeral Key Support

Good Ephemeral keys are used in some of the cipher suites your client supports. This means your client may be used to provide forward secrecy if the server supports it. This greatly increases your protection against snoopers, including global passive adversaries who scoop up large amounts of encrypted traffic and store them until their attacks (or their computers) improve.

Learn More

Session Ticket Support

Improvable Session tickets are not supported in your client. Without them, services will have a harder time making your client's connections fast. Generally, clients with ephemeral key support get this for free.

Learn More

TLS Compression

Good Your TLS client does not attempt to compress the settings that encrypt your connection, avoiding information leaks from the CRIME attack.

Learn More

BEAST Vulnerability

Good Your client is not vulnerable to the BEAST attack because it's using a TLS protocol newer than TLS 1.0. The BEAST attack is only possible against clients using TLS 1.0 or earlier using Cipher-Block Chaining cipher suites that do not implement the 1/n-1 record splitting mitigation.

Learn More

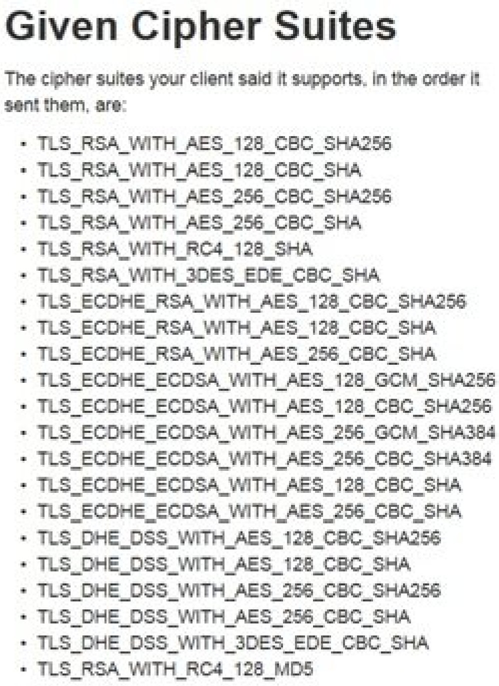
Insecure Cipher Suites

Bad Your client supports cipher suites that are known to be insecure:

- TLS_RSA_WITH_RC4_128_MD5: This cipher uses RC4 which has insecure biases in its output.
- TLS_RSA_WITH_RC4_128_SHA: This cipher uses RC4 which has insecure biases in its output.

Learn More

در پایین صفحه گزارشی از بستههای سایفری که توسط اینترنتاکسپلورر پشتیبانی میشود را مشاهده میکنید .



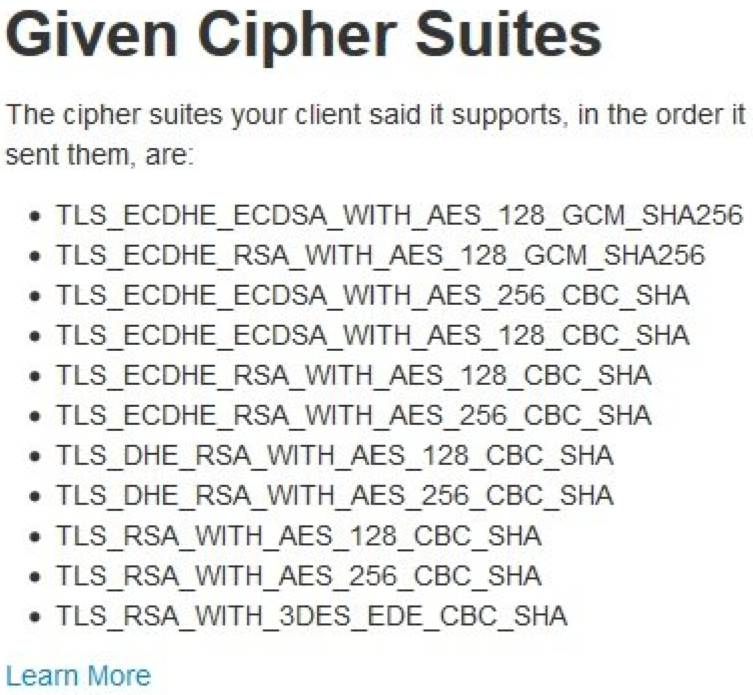
Given Cipher Suites

The cipher suites your client said it supports, in the order it sent them, are:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_RC4_128_MD5

فایرفاکس (نسخه **41.0.2** آزمایش شده)

اگر آدرس How’s My SSL را در مرورگر فایرفاکس اجرا کنیم، گزارش زیر را دریافت خواهیم کرد .



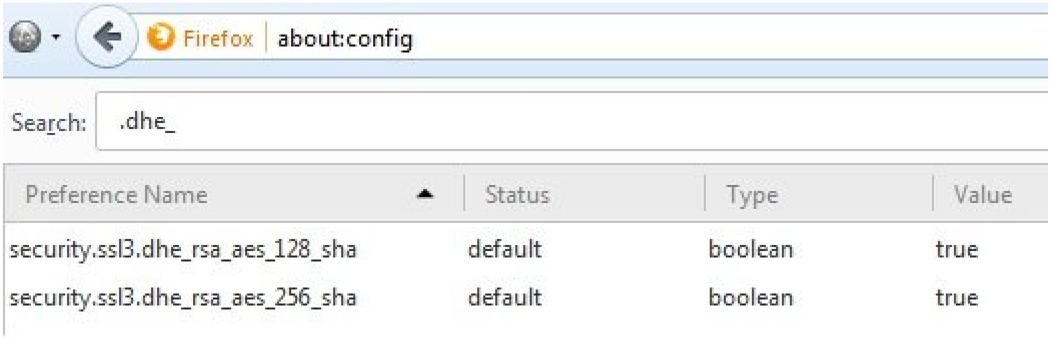
Given Cipher Suites

The cipher suites your client said it supports, in the order it sent them, are:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

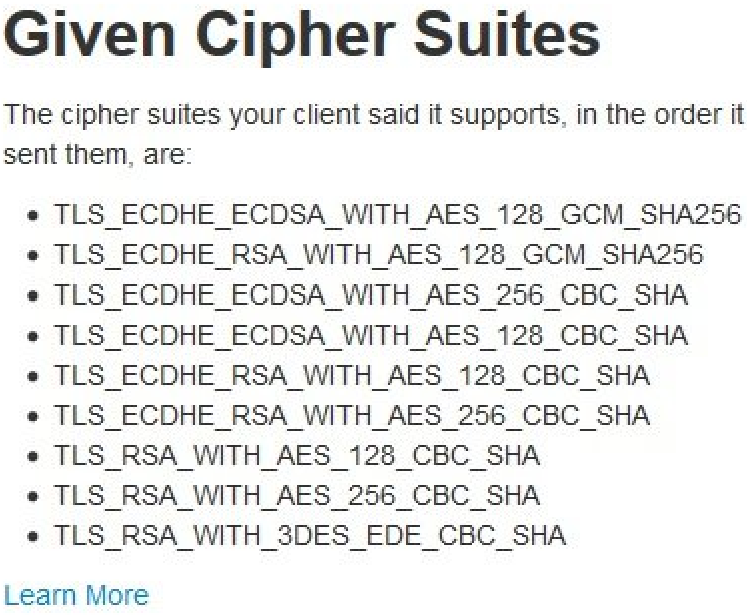
Learn More

ابتدا زبانه جدیدی باز کرده، عبارت about:config را در نوار آدرس تایپ کرده و کلید Enter را فشار دهید. در صفحه هشدار روی گزینه I’ll be careful, I promise! کلیک کنید . در نوار آدرس عبارت _dhe. را تایپ کرده و کلید Enter را فشار دهید . اجرای این دستور دو تنظیم security.ssl3.dhe_rsa_aes_256_sha و security.ssl3.dhe_rsa_aes_256_sha را در اختیارتان قرار میدهد . مقدار هر دو گزینه را از true به false تغییر دهید . برای این منظور روی هر یک از این گزینهها بهطور جداگانه دوبار کلیک کرده تا وضعیت آنها به false تغییر پیدا کند .



Preference Name	Status	Type	Value
security.ssl3.dhe_rsa_aes_128_sha	default	boolean	true
security.ssl3.dhe_rsa_aes_256_sha	default	boolean	true

اکنون صفحه How’s My SSL را یکبار نوسازی (Refresh) کنید . اکنون باید بسته _DHE_ از میان رفته باشد .



Given Cipher Suites

The cipher suites your client said it supports, in the order it sent them, are:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

مرورگر کروم

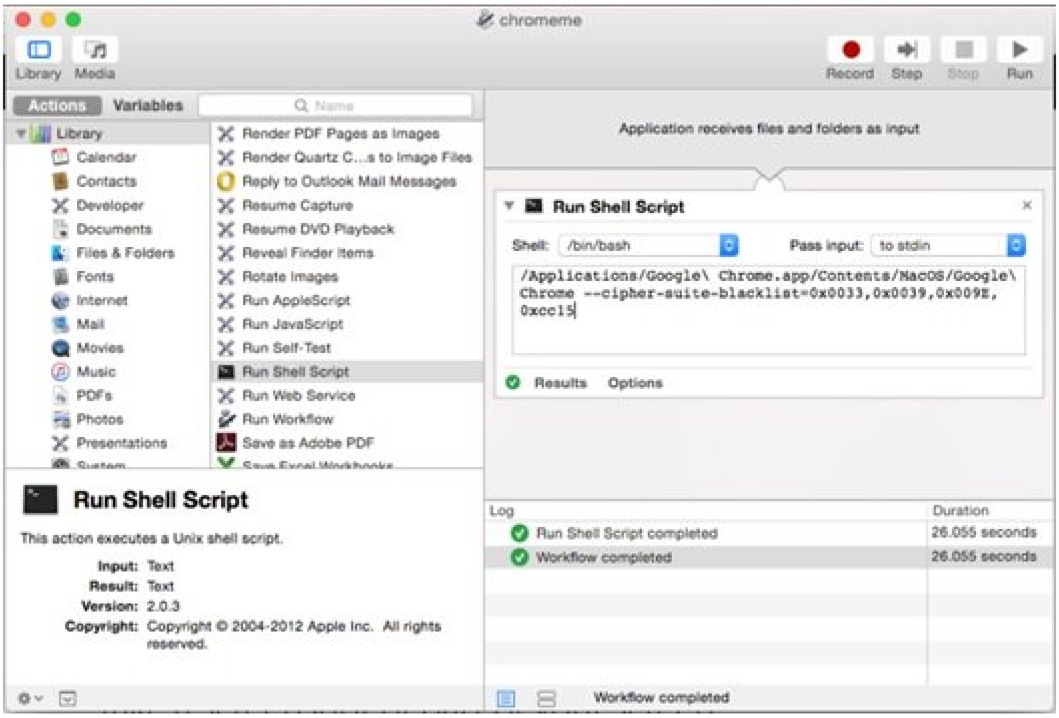
برای اطلاع از وضعیت امنیتی مرورگر کروم، در زبانه مرورگر خود صفحه How’s My SSL را باز کنید . نکتهای که در ارتباط با کروم باید به آن اشاره کرد به نحوه تغییر مقادیر باز میگردد . در مرورگر کروم مقادیر باید در فرمت هگزا (Hex) شانزدهی برای کروم ارسال شوند . برای مشاهده فهرست مربوطه به آدرس **TLS Cipher Suit Registry** مراجعه کنید .

اما نحوه تغییر وضعیت این مرورگر در سیستمعاملهای مختلف به شرح زیر است :

سیستمعامل **OSX** (نسخه های **46.0.2490.71** و **10.10.5** آزمایش شده اند)

Automator را باز کرده، روی Run Shell Script دوبار کلیک کنید . فرمان cat را مطابق دستور زیر جایگزین کنید :

```
Applications/Google\ Chrome.app/Contents/MacOS/Google\ Chrome --cipher-suite-/
blacklist=0x0033,0x0039,0x009E,0xcc15
```



chromeme
Library
Media
Record
Step
Stop
Run
Actions
Variables
Name
Library
Calendar
Contacts
Developer
Documents
Files & Folders
Fonts
Internet
Mail
Movies
Music
PDFs
Photos
Presentations
System
Render PDF Pages as Images
Render Quartz C...s to Image Files
Reply to Outlook Mail Messages
Resume Capture
Resume DVD Playback
Reveal Finder Items
Rotate Images
Run AppleScript
Run JavaScript
Run Self-Test
Run Shell Script
Run Web Service
Run Workflow
Save as Adobe PDF
Save Excel Workbooks
Results
Options

Application receives files and folders as input

Run Shell Script

Shell: /bin/bash

Pass input: to stdin

```
/Applications/Google\ Chrome.app/Contents/MacOS/Google\
Chrome --cipher-suite-blacklist=0x0033,0x0039,0x009E,
0xcc15
```

Run Shell Script

This action executes a Unix shell script.

Input: Text
Result: Text
Version: 2.0.3
Copyright: Copyright © 2004-2012 Apple Inc. All rights reserved.

```
Log                                  Duration
Run Shell Script completed           26.055 seconds
Workflow completed                   26.055 seconds
```

Workflow completed

برنامه را در پوشه برنامه کاربردی همراه با نام فایل دلخواهی ذخیره کنید . البته، میتوانید برنامه کاربردی را به سمت داک کشیده و از آنجا اقدام به اجرای کروم بدون استفاده از سایفر آسیبپذیر کنید .

سیستمعامل ویندوز (ویندوز 7 آزمایش شده)

روی میانبر مرورگر کروم در دسکتاپ کلیک راست کرده، گزینه Properties را انتخاب کنید . در ادامه برای سایفرهای فوق مقدار شانزدهی را همانگونه که پیشتر گفتیم وارد کنید .

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --cipher-suite-blacklist=0x0033,0x0039,0x009E,0xcc15

اکنون کروم را از طریق میانبر صفحه دسکتاپ اجرا کنید . سایفرهای مربوطه برداشته شدهاند .

سیستمعامل لینوکس (اوبونتو 14.04 LTS آزمایش شده)

کروم را از طریق خط فرمان اجرا کرده و بسته سایفر را همانند عبارت زیر از آن حذف کنید .

google-chrome --cipher-suite-blacklist=0x0033,0x0039,0x009E,0xcc15

پروتکل SSH

بعد از آنکه ثابت شد NSA توانایی رمزگشایی ارتباطات SSH را دارد، یک دستورالعمل عالی برای پیکربندی محکم SSH از سوی کارشناسان امنیتی منتشر شد . نحوه اجرای این دستورالعمل را از آدرس **Secure Secure Shell** میتوانید دریافت کنید .

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
18:12 - 16/09/1394
برچسب:
امنیت - مرورگر - دیفن_هلمن - رمزنگاری - فایرفاکس - کروم - How’s My SSL - SSH - VPN - HTTPS

نشانی منبع **:**https://www.shabakeh-mag.com/security/2060