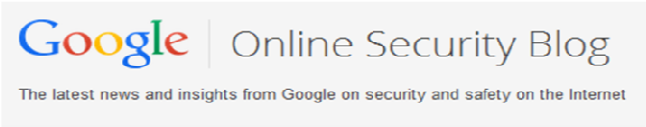
مقدمه

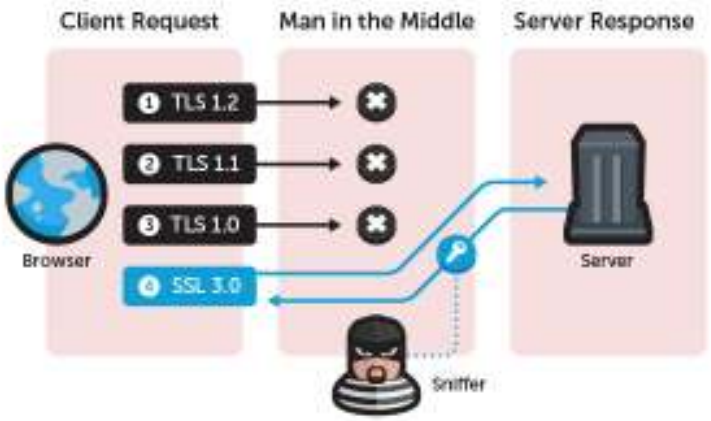
آسیب‌پذیری Poodle در تاریخ ۱۴ اکتبر ۲۰۱۴ توسط تیم امنیت اطلاعات شرکت گوگل منتشر اعلان شده است.



This POODLE bites: exploiting the SSL 3.0 fallback

این آسیب‌پذیری ناشی از مشکل در پیاده سازی پروتکل نیست بلکه از یک ضعف ذاتی در پروتکل SSLv3 سرچشمه می‌گیرد.بنابراین تنها راه برطرف کردن این آسیب‌پذیری، غیر فعال کردن کامل این پروتکل است. این آسیب‌پذیری به مهاجم این امکان را می‌دهد که از محتوای حساس کاربر در حین یک اتصال sslرمزگشایی نماید (به عنوان نمونه به اطلاعات هویتی در کوکی دسترسی پیدا کند). این امر امکان سواستفاده ازحساب های بانکی و... را فراهم می‌نماید.

SSLV3 یک پروتکل برای رمزنگاری ارتباط بین کلاینت و سرور است تا محتوای رد و بدلی بین آنها قابل مشاهده توسط بقیه نباشد. اما این پروتکل منسوخ و ناامن است (بیش از ۱۸ سال از عمر این پروتکل می‌گذرد). جایگزین این پروتکل TLS(Transport Layer Secure) می‌باشد که چنین ضعف ساختاری در برقراری ارتباط امن در آن وجود ندارد. اما در برقراری ارتباط امن بین client و Server و به منظور سازگاری با تمامی نسخه های مرورگرها، پروتکل های قدیمی‌تر همچنان پشتیبانی می‌گردند. بنابراین وقتی یک تلاش برای اتصال امن TLSبین client و server با مشکل روبرو می‌شود، سرور از پروتکل قدیمی‌تر مانند sslv3 استفاده می‌نماید. شخص مهاجم از این ویژگی استفاده کرده و در فرایند مذاکره بین client و server با شبیه سازیشرایطی که نشانگر عدم برقراری ارتباط امن بین client و server است، سرور را مجبور می‌کند از پروتکل SSLv3 استفاده نماید و آنگاه از ضعف ساختاری پروتکل SSLV3 با استفاده از حمله مرد میانی سودجویی می‌نماید.



شرایط اجرای حمله

به منظور بهره برداری موفق، مهاجم بایستی بتواند کدهای مخرب javascript را در مرورگر قربانی تزریق نماید. همچنین بایستی توانایی مشاهده و دستکاری ترافیک رمز شده را داشته باشد (در حقیقت بایستی شرایط حمله مرد میانی مهیا باشد).

شناسایی آسیب‌پذیری در مرورگر و سرور

- افراد عادی برای تست آسیب‌پذیری مرورگر خود می‌توانند به وب سایت زیر مراجعه کنند:

https://www.poodletest.com

- به منظور تست آسیب‌پذیری سرورها می‌توان به وب سایت زیر مراجعه نمود:

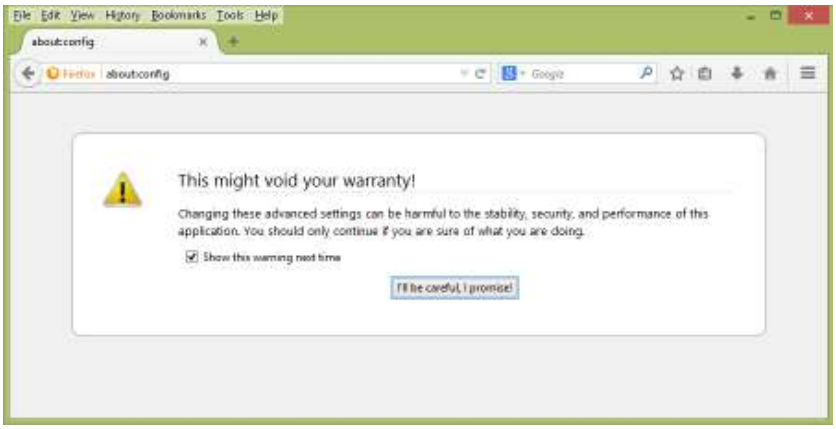
https://www.ssltest.com

راه‌کارهایی برای جلوگیری از سوءاستفاده از آسیب‌پذیری پودل

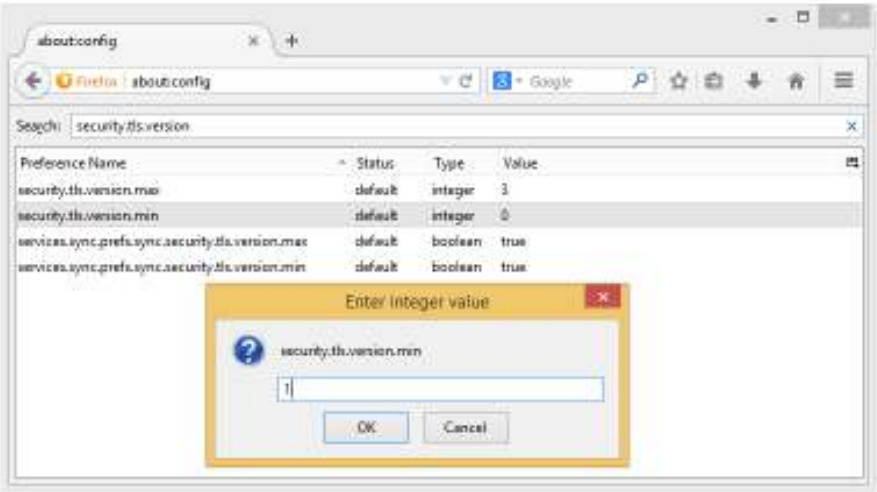
به منظور برطرف سازی این آسیب‌پذیری، راه حل اساسی از کار انداختن پروتکل SSLV3 بر روی مرورگر و سرور است. در ادامه نحوه غیرفعال کردن SSLV3 بر روی سرورها و مرورگرهای مختلف نشان داده شده است.

مرورگر فایرفاکس

با وارد کردن about:config در نوار آدرس، صفحه زیر مشاهده خواهد شد.



گزینه I'll be careful, I Promise! را اتخاب نموده و سپس در نوار جستجو مقدار security.tls.version را وارد می‌نماییم. با انجام این کار، چهار مقدار نمایش داده خواهند شد (شکل زیر). حال کافی است که مقدار value را برای security.tls.version.min برابر با ۱ قرار داد.

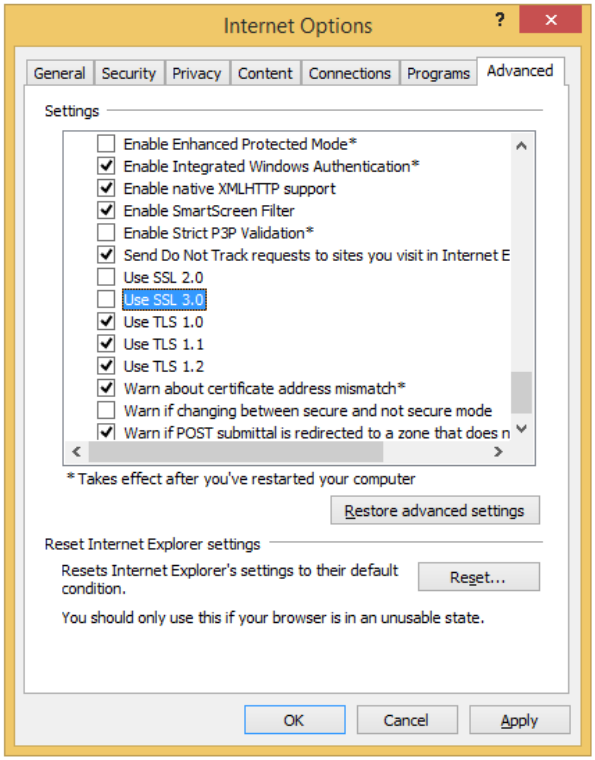


مرورگر گوگل کروم

با راست کلیک بر روی آیکن مرورگر و ورود به بخش propertiesو سپس وارد نمودن دستور --ssl-version-min=tls1 در انتهای مسیر (قسمت مشخص شده در شکل)، می‌توان موجب غیرفعال سازی SSL بر روی مرورگر شد.

مرورگر اینترنت اکسپلورر

در مسیر Tools/Internet Options/Advanced بایستی گزینه Use SSL 3.0 غیرفعال گردد:



همچنین در مقاله [1] به استفاده از شاخص TLS_FALLBACK_SCSVبرای جلوگیری از استفاده از پروتکل‌های قدیمی‌تر (مانند sslv3)در زمان عدم برقراری ارتباط بین کلاینت و سرور اشاره شده است.

شرکت گوگل این ویژگی را در گوگل کروم و وب سایت خود از ماه February امسال پیاده‌سازی کرده است. فایرفاکس نیز اعلام کرده این شاخص را در ابتدای سال ۲۰۱۵ پیاده سازی خواهد کرد.

غیرفعال سازی SSLV3 در سمت سرور

Apache

The SSL configuration file changed slightly in httpd version 2.2.23. For httpd version 2.2.23 and newer, specify all protocols except SSLv2 and SSLv3.

```
SSLProtocol ALL -SSLv2 -SSLv3
```

For httpd version 2.2.22 and older, only specify TLSv1. This is treated as a wildcard for all TLS versions.

```
SSLProtocol TLSv1
```

For Apache + mod_nss, edit `/etc/httpd/conf.d/nss.conf` to allow only TLS 1.0+.

```
NSSProtocol TLSv1.0,TLSv1.1
```

به منظور غیرفعال سازی sslv3 بر روی IISمی‌توانید به آدرس زیر مراجعه کنید:

https://www.digicert.com/ssl-support/iis-disabling-ssl-v3.htm