آسیب پذیری FREAK و ارایه راهکارهای رفع آسیب پذیری

در تاریخ ۳ مارچ ۲۰۱۵، آسیب پذیری جدید SSL/TLS با نام حمله FREAK(CVE 2015-0204) معرفی گردید.این آسیب پذیری به مهاجم امکان می دهد بین ارتباط HTTPS کاربران و سرورهای آسیب پذیر قرار گیرد و آن ها را مجبور به استفاده از رمزنگاری ضعیف تر نماید، در نتیجه اطلاعات حساس دستکاری یا سرقت خواهد شد. با توجه به این که تعداد بسیار بالایی از سایت ها در دنیا و در ایران دارای این آسیب پذیری هستند لذا لازم است هرچه سریع تر نسبت به رفع آن اقدام گردد. علاوه بر سرورهای آسیب پذیر، Akamai هم میزبان تعداد بسیار بالای از سایت های آسیب پذیر بوده است که از آن هامی توان به facebook و FBI اشاره کرد. این وب سایت ها بی درنگ نسبت به رفع آن اقدام نمودند.

نسخه های آسیب پذیر

کتابخانه های TLS client آسیب پذیر به شرح ذیل است:

OpenSSL(CVE-2015-0204): نسخه های قبل از 1.0.1k آسیب پذیر هستند.

BoringSSL: نسخه های قبل از ۱۰ نوامبر ۲۰۱۴ آسیب پذیر هستند.

LibReSSL: نسخه های قبل از 2.1.2 آسیب پذیر هستند.

SecureTransport: آسیب پذیر است و راه حل در راه بررسی است.

SChannel: آسیب پذیر است[1]. راه حل در حال بررسی است

Mono: نسخه های قبل از 3.12.1 آسیب پذیر هستند

IBM JSSE: آسیب پذیر است و راه حل در راه بررسی است.

مرورگرهای وب که از کتابخانه های TLS بالا استفاده می کنند، آسیب پذیر هستند، شامل:

Chrome: نسخه های قبل از 41 آسیب پذیر هستند. آن را به Chrome 41 بروزرسانی کنید.

Internet Explorer: آسیب پذیر است. منتظر وصله برای رفع آسیب پذیری هستیم.

[1] https://technet.microsoft.com/en-us/library/security/3046015

Safari: آسیب پذیر است. منتظر وصله برای رفع آسیب پذیری هستیم.

Android Browser: آسیب پذیر است. آن را به Chrome 41 بروزرسانی کنید.

Blackberry Browser: آسیب پذیر است. منتظر وصله برای رفع آسیب پذیری هستیم.

Opera: روی Mac و Android آسیب پذیر است. آن را به Opera 28 بروزرسانی کنید.

دیگر برنامه های کاربردی client(مانند email) که از کتابخانه های TLS آسیب پذیر استفاده می کنند هم آسیب پذیر هستند.

نحوه شناسایی آسیب پذیر بودن:

با استفاده از وب سایت های ذیل می تواند آسیب پذیر بودن سایت خود را شناسایی کنید:

https://tools.keycdn.com/freak

https://www.ssllabs.com/ssltest

نحوه رفع آسیب پذیری

اگر سرور دارید:

شما بایستی فوراً پشتیبانی از کتابخانه های رمزنگاری TLS export را غیرفعال کنید. درحالی که در آن هستید شما باید دیگر مجموعه که ناامن شناخته شده اند غیرفعال و انتقال امن را فعال کنید. برای شناخت چگونگی امن سازی نرم افزار سرور HTTPS می توانید به راهنمای تنظیمات امنیتی موزیلا[2] و تولید کننده تنظیمات SSL[3] مراجعه کنید.برای تست تنظیمات و اطمینان از آسیب پذیر نبودن می توانید از لینک های قسمت قبل استفاده کنید.

اگر از مرورگر استفاده می کنید:

اطمینان حاصل کنید که از آخرین نسخه های مرورگرها و بروزرسانی آن ها استفاده کرده اید.

اگر مدیرسیستم یا توسعه دهنده هستید:

[2] https://wiki.mozilla.org/Security/Server_Side_TLS#Recommended_configurations
[3] https://mozilla.github.io/server-side-tls/ssl-config-generator/

اطمینان حاصل کنید نسخه های کتابخانه TLSمورد استفاده شما بروز باشد. OpenSSL، Microsoft Schannel و AppleSecureTransport که وصله جدید ندارند، هنوز آسیب پذیرند. توجه کنید که این کتابخانه ها مورد استفاده برخی از برنامه ها مانند wget و curl هم هست. شما همچنین باید اطمینان حاصل کنید که نرم افزار شما exportکتابخانه های رمزنگاری را پیشنهاد ندهد، حتی اگر به عنوان آخرین راه حل باشد. چون در این صورت ممکن است حتی را در صورت وصله شدن کتابخانه TLS مورد سوء استفاده قرار گیرد. در لینک https://freakattack.com/clienttest.htmlابزارهایی برای توسعه دهندگان نرم افزار که برای تست مفید است قرار داده شده است[4].

[4]https://freakattack.com/clienttest.html