FREAK

Security Advisory

FREAK Attack (CVE-2015-0204; CVE-2015-1637)

OVERVIEW

A recently-identified critical security issue, FREAK[1], allows an attacker in a privileged network position to intercept and decrypt TLS-protected network traffic between certain vulnerable TLS client libraries, and servers that are configured to support export-grade cipher suites.

Export-grade cipher suites make use of deliberately weakened encryption keys in order to comply with 1990s-era United States laws that restricted the export of strong cryptography. They exist solely for the purpose of complying with antiquated laws, and were deprecated after these laws were relaxed in 2000. The 512-bit RSA keys used by export-grade cipher suites are easily broken using today's computer hardware and cloud services. Export-grade cipher suites should never be used; most web browsers and other TLS *clients* ship with these suites disabled by default, but some *servers* still have them enabled for backward compatibility with obsolete clients that only support export-grade cryptography.

The FREAK attack leverages a vulnerability in certain TLS libraries, including OpenSSL and Apple SecureTransport, to downgrade the connection from strong cryptography to export-grade cryptography by performing a man-in-the-middle attack. Specifically, when the client opens the connection and sends a ClientHello message listing the cipher suites it supports, the adversary replaces the list with export-grade cipher suites only. This causes the server to present a 512-bit RSA key to the client for the purposes of key exchange, and due to implementation bugs, OpenSSL, Apple SecureTransport, and Microsoft Schannel fail to check to see whether export-grade encryption is enabled in their configurations before accepting and using the weakened key.

The adversary must then break the 512-bit RSA encryption used in the key exchange process in order to decrypt the underlying traffic. Security researchers estimate that a 512-bit RSA public key can be factored in 7.5 hours[2], allowing the adversary to derive the corresponding private key. Given the server's 512-bit RSA key pair, and recorded network traffic from a TLS connection successfully downgraded to export-grade cryptography, an adversary can use the RSA private key to decrypt the key exchange message sent during the handshake process, and then decrypt all traffic sent over the connection.

ATTACK REQUIREMENTS

- The attacker must have the ability to intercept and modify network traffic between the client and server, i.e., the attacker must be in an active man-in-the-middle position.
- The client software must rely on a TLS library vulnerable to FREAK, such as OpenSSL, Apple SecureTransport, or Microsoft Schannel.
- The server must have support for export-grade cipher suites enabled.

AFFECTED CLIENTS

- All versions of OpenSSL prior to 0.9.8
- OpenSSL 0.9.8 series, prior to version 0.9.8zd

[1] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204
[2] http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html

- OpenSSL 1.0.0 series, prior to version 1.0.0p
- OpenSSL 1.0.1 series, prior to version 1.0.1k
- All versions of Apple SecureTransport. As of this writing, Apple has not released a patch.
- All versions of Windows Schannel[3]. As of this writing, Microsoft has not released a patch.

The built-in Android browser, Apple Safari for iOS and Mac OS X, as well as Microsoft Window's Internet Explorer are vulnerable to FREAK.

Web browsers can be tested for susceptibility to FREAK using a test website available at https://freakattack.com/. However, **any** software making use of a vulnerable TLS library will also be vulnerable.

AFFECTED SERVERS

The FREAK attack requires that a server have export-grade cryptography enabled.

A given TLS server, such as *www.google.com* on port 443, can be tested for support of export-grade cipher suites using the OpenSSL command line utility:

```
openssl s_client -connect www.google.com:443 -cipher EXP < /dev/null
```

If this command results in an error message, the server refused to connect using export-grade encryption. If the connection succeeds and OpenSSL displays the word DONE on the screen, then the server allows export-grade encryption and is susceptible to the FREAK attack.

RECOMMENDATIONS

- Export-grade cipher suites should be disabled on all web or other servers using TLS-based encryption. ISE has previously published a blog[4] post that contains recommendations for selecting appropriate cipher suites.
- Software vendors who use and bundle a copy of OpenSSL with their applications should immediately upgrade to OpenSSL 0.9.8zd, 1.0.0p, or 1.0.1k[5].
- Linux distributions or other products containing a bundled copy of OpenSSL should be updated with the latest vendor security patches.
- Apple Mac OS X or iOS devices should be updated with the latest vendor security patches, once Apple releases a patched version of SecureTransport.
- Windows machines should be updated with the latest vendor security patches, once Microsoft releases a patched version of Schannel.

MORE DETAILS

Full technical details about the FREAK attack are available from the following resources:

- https://www.smacktls.com/
- http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html

[3] https://technet.microsoft.com/en-us/library/security/3046015
[4] http://securityevaluators.com/knowledge/blog/20150119-protocols/
[5] https://www.openssl.org/news/secadv_20150108.txt