Vulnerabilities in SSL & TLS

ATTACK	CVE	AFFECTS	MITIGATION
Logjam	CVE-2015-4000	The TLS protocol 1.2 and earlier when a DHE_EXPORT cipher suite is enabled.	Enforce DH group sizes of 1,024 bits and above
POODLE	CVE-2014-3566	SSL version 3.0	Disable support for SSL 3.0
BEAST	CVE-2011-3389	TLS 1.0 or any version of SSL	Enforce TLS 1.1 and higher
CRIME	2012-4929	TLS compression	Disable TLS compression
BREACH and TIME	CVE-2013-3587	HTTP compression	Disable HTTP compression
Lucky 13	CVE-2013-0169	TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2 in several vendors products	Disable CBC ciphers if your server implementation is flawed
RC4 byte biases	CVE-2013-2566	Connections supporting RC4	Disable support for RC4 cipher suites
FREAK	CVE-2015-0204	Any system willing to negotiate RSA Export	Disable support for weak export-grade ciphers
SWEET32	CVE-2016-2183 and CVE-2016-6329	Long term client browser foot hold	Do not support or negotiate 3DES cipher-suites. At a minimum, AES should be preferred over 3DES. Limit length of TLS session.

EVILSAINT