Tracking the FREAK Attack

On Tuesday, March 3, 2015, researchers announced a new SSL/TLS vulnerability called the FREAK attack. It allows an attacker to intercept HTTPS connections between vulnerable clients and servers and force them to use weakened encryption, which the attacker can break to steal or manipulate sensitive data. This site is dedicated to tracking the impact of the attack and helping users test whether they're vulnerable.

The FREAK attack was discovered (http://smacktls.com) by Karthikeyan Bhargavan (http://prosecco.inria.fr/personal/karthik) at INRIA in Paris and the miTLS team (http://mitls.org). Further disclosure was coordinated by Matthew Green (http://blog.cryptographyengineering.com/). This report is maintained by computer scientists at the University of Michigan, including Zakir Durumeric (https://zakird.com/), David Adrian (https://davidadrian.org/), Ariana Mirian, Michael Bailey (http://mdbailey.ece.illinois.edu/), and J. Alex Halderman (https://jhalderm.com/). The team can be contacted at freakattack@umich.edu (mailto:freakattack@umich.edu).

For additional details about the attack and its implications, see this post by Matt Green (http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html), this site by the discoverers (https://www.smacktls.com/), this Washington Post article (http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/03/freak-flaw-undermines-security-for-apple-and-google-users-researchers-discover/), and this post by Ed Felten (https://freedom-to-tinker.com/blog/felten/freak-attack-the-chickens-of-90s-crypto-restriction-come-home-to-roost/).

Who is vulnerable?

The FREAK attack is possible when a vulnerable browser connects to a susceptible web server—a server that accepts "export-grade" encryption.

Servers

Servers that accept RSA_EXPORT cipher suites put their users at risk from the FREAK attack. Using Internet-wide scanning, we have been performing daily tests of all HTTPS servers at public IP addresses to determine whether they allow this weakened encryption. More than a third of all servers with browser-trusted certificates are at risk.

	Currently Vulnerable	Change Since Mar. 3
HTTPS servers at Alexa (http://www.alexa.com/topsites) Top 1 Million domain names	8.5%	down from 9.6%
HTTPS servers with browser-trusted certificates	6.5%	down from 36.7%
All HTTPS servers	11.8%	down from 26.3%

See below for a list of vulnerable popular domains. You can test servers using the SSL FREAK Check (https://tools.keycdn.com/freak) tool or the Qualys SSL Labs' SSL Server Test (https://www.ssllabs.com/ssltest/), which can also identify other security problems.

Clients

Update (Mar. 5): Browsers are vulnerable to the FREAK attack because of bugs that allow an attacker to force them to use weak, export-grade encryption. One example is the OpenSSL bug described in CVE-2015-0204 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204), but some other TLS libraries have similar problems. Far more browsers are vulnerable to the FREAK attack than was initially thought when the attack was announced, including:

Patch available now

Vulnerable Browser	Status
Internet Explorer	Patch available now (https://technet.microsoft.com/en-US/library/security/MS15-031) — Security advisory (https://technet.microsoft.com/en-us/library/security/3046015)
Chrome on Mac OS	Patch available now
Chrome on Android	Patch available now
Safari on Mac OS	Patch available now (https://support.apple.com/en-us/HT204413)
Safari on iOS	iOS 8 Patch available now (https://support.apple.com/en-us/HT204423)
Stock Android Browser	
Blackberry Browser	
Opera on Mac OS	Patch available now

You can check whether your browser is vulnerable using our **FREAK Client Test Tool (clienttest.html)**.

Chrome for Windows and all modern versions of Firefox are known to be safe. However, even if your browser is safe, certain third-party software, including some anti-virus products and adware programs, can expose you to the attack by intercepting TLS connections from the browser. If you are using a safe browser but our client test says you're vulnerable, this is a likely cause.

In addition to browsers, many mobile apps, embedded systems, and other software products also use TLS. These are also potentially vulnerable if they rely on unpatched libraries or offer RSA_EXPORT cipher suites.

What should I do?

If you run a server ...

You should immediately disable support for TLS export cipher suites. While you're at it, you should also disable other cipher suites that are known to be insecure and enable forward secrecy. For instructions on how to secure popular HTTPS server software, we recommend Mozilla's security configuration guide (https://wiki.mozilla.org/Security/Server_Side_TLS#Recommended_configurations) and their SSL configuration generator (https://mozilla.github.io/server-side-tls/ssl-config-generator/). We also recommend testing your configuration with the Qualys SSL Labs SSL Server Test (https://www.ssllabs.com/ssltest/) tool.

If you use a browser ...

Make sure you have the most recent version of your browser installed, and check for updates frequently. Updates that fix the FREAK attack should be available for all major browsers soon.

If you're a sysadmin or developer ...

Make sure any TLS libraries you use are up to date. Unpatched OpenSSL (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204), Microsoft Schannel (https://technet.microsoft.com/en-us/library/security/3046015), and Apple SecureTransport all suffer from the vulnerability. Note that these libraries are used internally by many other programs, such as `wget` and `curl`. You also need to ensure that your software does not offer export cipher suites, even as a last resort, since they can be exploited even if the TLS library is patched. We have provided tools for software developers (clienttest.html) that may be helpful for testing.

Popular sites that are susceptible to FREAK

The following sites from the Alexa (http://www.alexa.com/topsites) Top 10,000 websites permit RSA_EXPORT cipher suites, which potentially puts their users at risk from the FREAK attack. This list is current as of March 10 at 8:00 AM EST. We urge these sites to drop support for export cipher suites as soon as possible.

Alexa Rank	Domain	Address Tested
55	ziddu.com	84.45.63.57
164	coccoc.com	123.30.175.29
227	ppomppu.co.kr	110.45.151.210
265	groupon.com	184.26.43.170
273	jabong.com	23.203.7.176
446	4shared.com	208.88.224.138
453	npr.org	216.35.221.76
601	airtel.in	125.19.135.93
615	kohls.com	23.202.240.45
722	adplxmd.com	205.186.187.178
740	tinyurl.com	23.194.152.87
784	mit.edu	23.6.64.128
798	saramin.co.kr	182.162.86.29
831	suning.com	112.84.133.57
865	itau.com.br	172.224.255.170
913	huaban.com	60.191.100.98
937	vi-view.com	50.97.32.135
1040	jobrapido.com	46.105.106.82
1093	wiocha.pl	195.225.138.230
1107	axisbank.com	119.226.139.40
1209	jcpenney.com	23.202.220.215
1247	mgid.com	208.94.232.200
1259	globososo.com	184.173.140.162
1301	binaryprofessional.com	50.7.157.122
1303	refinery29.com	50.22.34.142
1332	vente-privee.com	185.45.180.3
1336	wowhead.com	23.6.67.58

Alexa Rank	Domain	Address Tested
1369	dhgate.com	124.42.15.198
1370	adxcore.com	188.165.36.101
1495	estadao.com.br	23.6.72.37
1543	sweet-page.com	50.97.32.133
1556	jcrew.com	23.199.196.136
1565	zdnet.com	50.112.160.88
1569	bmi.ir	89.235.64.67
1658	cornell.edu	128.253.173.244
1663	vesti.ru	80.247.32.206
1665	uludagsozluk.com	188.132.225.181
1671	lg.com	165.244.62.23
1702	umich.edu	141.211.243.44
1780	extra.com.br	23.194.154.91
1791	ibtimes.co.uk	64.147.114.55
1835	syosetu.com	111.64.91.10
1852	jiameng.com	117.78.2.204
1871	thrillist.com	50.57.33.153
1885	dealmoon.com	198.23.88.242
1891	ihg.com	23.202.251.213
1899	mashreghnews.ir	94.182.146.23
1920	ohmyzip.com	216.176.192.139
1925	alice.it	217.169.121.227
1955	duba.com	114.112.93.100
1962	ana.co.jp	202.224.1.7
1973	gg.com.ua	213.227.192.135
1986	miui.com	42.62.48.148
1999	copyscape.com	212.100.239.219

Alexa Rank	Domain	Address Tested
2017	accountonline.com	192.193.8.101
2028	timesjobs.com	115.112.206.11
2061	eltiempo.com	200.41.9.39
2077	leparisien.fr	95.131.142.225
2110	epnet.com	140.234.254.41
2132	bigrock.in	103.21.58.212
2143	delfi.lt	91.234.200.110
2161	pontofrio.com.br	23.193.175.4
2215	unam.mx	132.248.10.44
2227	indiocasino.com	212.64.147.151
2235	gobizkorea.com	211.119.134.217
2302	sedo.com	82.98.86.183
2308	jstor.org	198.108.24.38
2357	doctissimo.fr	85.116.34.4
2361	wannonce.com	188.165.15.58
2377	lolking.net	23.6.67.58
2391	56.com	59.32.213.232
2399	itv.com	193.35.9.65
2403	incruit.com	121.254.160.232
2411	rotoworld.com	64.210.192.54
2418	famitsu.com	202.90.182.200
2421	mafengwo.cn	119.254.76.148
2430	tradeindia.com	14.140.161.58
2519	taikang.com	116.58.220.1
2701	dailybasis.com	68.169.73.82
2709	beitaichufang.com	182.18.17.202
2720	eleconomista.es	217.116.23.3

Alexa Rank	Domain	Address Tested
2727	suntimes.com	64.94.90.42
2740	talktalk.co.uk	62.24.150.2
2756	mk.co.kr	220.73.139.201
2780	made-in-china.com	72.32.82.237
2802	337.com	174.36.254.166
2804	twitcasting.tv	202.234.23.144
2822	gocomics.com	66.6.101.183
2835	casasbahia.com.br	23.194.147.107
2842	hotelurbano.com	54.174.71.24
2877	giga.de	80.86.80.168
2883	marksandspencer.com	23.203.7.229
2907	coolenjoy.net	222.237.78.174
2952	seobook.com	207.97.249.100
2967	weathernews.jp	203.216.211.69
2995	www.net.cn	42.156.140.7
3100	olleh.com	183.110.184.90
3114	sidereel.com	173.247.105.225
3116	nsw.gov.au	203.3.232.71
3164	motorola.com	144.188.128.101
3178	infibeam.com	180.179.101.143
3236	usajobs.gov	23.47.34.35
3237	santander.com.br	172.224.248.145
3240	wechat.com	203.205.142.141
3272	ehanex.com	203.251.153.26
3303	sbicard.com	14.140.196.129
3346	jorudan.co.jp	210.168.27.165
3351	1hai.cn	222.73.36.200

Alexa Rank	Domain	Address Tested
3382	enuri.com	124.243.126.244
3416	afreeca.com	121.125.76.89
3451	hola.com	62.22.171.50
3461	trafficshop.com	78.140.142.21
3483	khan.co.kr	203.234.148.252
3502	19lou.com	115.236.99.92
3535	afkarnews.ir	5.144.129.189
3550	icbc.com.cn	202.99.30.211
3588	lenskart.com	54.254.151.162
3599	delfi.lv	62.63.137.4
3601	yinyuetai.com	117.79.131.138
3621	pc6.com	218.6.111.42
3638	persianv.com	5.144.130.216
3680	dominos.co.in	202.87.34.218
3695	honda.com	164.109.25.194
3699	kuwo.cn	221.238.18.58
3703	wmmail.ru	185.15.210.21
3711	tribalfusion.com	204.11.109.195
3714	am15.net	144.76.226.147
3744	dinodirect.com	184.173.225.136
3761	nordstromrack.com	23.193.174.147
3783	mediaite.com	69.60.14.234
3792	standardbank.co.za	196.8.136.20
3796	hypebeast.com	50.112.144.237
3979	backlinkwatch.com	74.204.189.20
4041	juntadeandalucia.es	217.12.24.33
4088	lan.com	67.15.147.205

Alexa Rank	Domain	Address Tested
4092	sec.gov	23.203.5.89
4099	gingersoftware.com	173.231.146.230
4100	marketgid.com	87.242.88.80
4195	nespresso.com	91.209.84.237
4206	gearbest.com	50.97.75.179
4240	key-find.com	50.97.32.136
4248	rincondelvago.com	198.64.137.53
4291	cjmall.com	210.122.101.150
4322	topshop.com	23.194.147.74
4345	delfi.ee	185.20.100.249
4379	pearson.com	159.182.33.151
4382	funweek.it	151.1.71.171
4383	linkprice.com	222.236.44.131
4440	virtualedge.com	74.205.242.20
4453	yes24.com	61.111.13.101
4454	pcfaster.com	180.76.2.25
4456	veoh.com	69.167.127.57
4467	ets.org	144.81.88.152
4491	rs-online.com	80.169.5.117
4531	alternet.org	198.16.5.137
4557	ria.com	213.95.148.25
4558	mamaclub.com	61.64.53.205
4591	lefrecce.it	23.194.156.12
4592	sofmap.com	61.204.171.132
4624	propellerads.com	78.140.145.202
4677	entekhab.ir	94.182.146.40
4697	eldiario.es	37.46.75.24

Alexa Rank	Domain	Address Tested
4725	pearltrees.com	93.184.35.40
4744	gongkong.com	59.151.1.94
4746	subscribe.ru	81.9.34.190
4753	e-rewards.com	63.241.211.118
4767	sleazyneasy.com	68.169.101.206
4803	kaixin001.com	220.181.103.141
4880	ip138.com	61.140.13.81
4884	katestube.com	64.188.53.206
4960	nova.cz	88.86.114.130
4962	usnetads.com	74.208.192.200
4987	filmstarts.de	62.39.143.50
4992	mangocity.com	121.34.253.140
5015	hostgator.in	103.21.59.167
5082	youmaker.com	64.62.138.65
5135	ohio.gov	156.63.96.228
5136	jahannews.com	87.107.52.140
5153	dereferer.org	195.234.228.80
5169	fishmpegs.com	68.169.73.82
5197	googleping.com	208.109.97.183
5248	trafficholder.com	64.111.214.2
5284	markt.de	213.95.6.42
5368	alriyadh.com	89.189.232.23
5446	gem.pl	85.232.225.226
5587	voici.fr	89.31.150.122
5650	orange.es	62.36.20.46
5671	lufax.com	211.95.2.97
5757	techgig.com	115.112.206.15

Alexa Rank	Domain	Address Tested
5824	vikatan.com	180.150.140.172
5855	umeng.com	211.151.151.6
5941	porsche.com	84.21.48.97
5956	designspiration.net	64.207.147.221
5960	draftkings.com	23.203.3.237
5972	alltop.com	184.106.130.115
5977	startlap.com	77.111.91.52
5978	canadiantire.ca	205.210.17.105
5991	33lc.com	183.136.217.16
6002	seoul.co.kr	211.169.247.231
6018	labirint.ru	194.84.83.148
6024	83suncity.com	122.152.179.70
6034	24ur.com	91.202.65.130
6051	sciencealert.com	119.81.53.4
6052	germanbankersecrets.org	50.7.157.122
6054	dreammail.jp	106.186.45.12
6056	dir.bg	194.145.63.12
6061	yootheme.com	188.226.251.160
6095	elnuevodia.com	196.32.153.146
6135	game321.com	37.58.67.11
6164	totheglory.im	38.83.103.226
6371	auto-profit-replicator.com	198.154.200.85
6443	hanjin.co.kr	203.251.153.29
6448	cr173.com	218.6.111.42
6478	infor.pl	193.164.157.245
6495	findthebest.com	50.18.121.78
6526	beyazperde.com	62.39.143.50

Alexa Rank	Domain	Address Tested
6564	stamps.com	216.52.211.93
6622	mps.it	195.7.19.86
6648	makeupalley.com	69.60.134.134
6715	leggo.it	85.18.214.165
6732	plan-q-secret.com	188.165.35.54
6745	rtl.be	81.92.238.91
6772	cue-monitor.jp	210.227.82.43
6774	wsodownloads.info	185.66.140.67
6819	femina.hu	195.228.155.84
6833	ad-center.com	208.99.88.30
6860	soaindo.com	119.81.21.170
6893	todaysppc.com	61.100.186.155
6984	correos.es	193.148.158.218
7006	daniweb.com	74.53.219.188
7037	nissan.co.jp	150.63.3.21
7039	myfxbook.com	108.163.193.212
7072	rzeczpospolita.pl	217.149.245.170
7079	savenkeep.com	81.88.48.82
7099	advego.ru	95.163.127.68
7123	trojmiasto.pl	193.104.50.210
7252	themarysue.com	69.60.24.234
7257	freedigitalphotos.net	95.138.157.18
7304	lordandtaylor.com	69.10.139.22
7345	geeksforgeeks.org	119.18.54.25
7360	madewell.com	23.202.222.232
7400	uninstallmaster.com	50.97.32.152
7412	planalto.gov.br	189.9.37.9

Alexa Rank	Domain	Address Tested
7426	dip.jp	61.197.187.238
7529	telenet.be	84.116.34.18
7545	hellomagazine.com	62.22.15.85
7566	subtitles.at	212.124.121.146
7581	fbdownloader.com	54.245.81.123
7608	copytraderpro.com	50.7.157.122
7629	brown.edu	128.148.252.129
7668	ripoffreport.com	192.225.215.36
7711	n4hr.com	184.173.179.185
7722	vw.com.tr	217.68.221.221
7730	minijuegos.com	217.13.124.222
7758	deser.pl	80.252.0.132
7766	calcalist.co.il	192.115.80.66
7774	5pao.com	125.90.204.47
7775	coach.com	23.202.227.155
7796	linksys.com	66.161.11.90
7813	networksolutionsemail.com	205.178.146.50
7818	qianxs.com	211.144.120.28
7841	wikimart.ru	195.208.182.2
7859	nielsen.com	138.108.20.122
7872	coocan.jp	202.248.237.141
7889	cnsnews.com	199.175.56.184
7895	chanet.com.cn	211.151.83.246
7915	streetdirectory.com	54.169.90.138
7944	davidsbridal.com	208.74.49.181
7955	eurobank.gr	193.58.70.3
7963	priberam.pt	62.28.135.67

Alexa Rank	Domain	Address Tested
7985	themalaysianinsider.com	203.223.159.194
8008	x3xtube.com	64.111.213.29
8017	gyakorikerdesek.hu	91.198.131.12
8019	jeep.com	129.9.76.228
8024	vno.co.kr	121.162.155.183
8035	macmillandictionary.com	195.138.194.22
8099	gaymaletube.com	64.188.56.183
8107	rzd.ru	217.175.140.90
8163	newsen.com	27.1.17.140
8165	netcombo.com.br	201.6.19.16
8220	escapadarural.com	176.31.247.181
8221	lyricsmode.com	178.18.22.163
8247	pinkvilla.com	174.129.200.25
8286	sensacine.com	62.39.143.50
8308	element14.com	83.100.177.204
8373	ucr.edu	138.23.226.208
8388	unext.jp	125.63.43.46
8455	restorationhardware.com	23.202.240.45
8479	yengo.com	27.254.59.193
8485	lfmall.co.kr	121.50.21.220
8531	jn.pt	80.251.169.144
8568	gordonua.com	91.224.10.20
8601	bluetradingonline.net	50.7.157.122
8652	wordtracker.com	148.251.89.68
8660	mbusa.com	141.113.146.23
8685	ui.ac.id	152.118.24.181
8734	ynetnews.com	192.115.80.66

Alexa Rank	Domain	Address Tested
8745	parsine.com	94.182.146.66
8779	photo.net	64.95.64.39
8794	baharnews.ir	87.107.133.77
8813	omniboxes.com	50.97.32.151
8847	senate.gov	23.202.229.166
8851	diegrossechance.net	50.7.157.122
8870	deichmann.com	145.253.207.220
8875	iesa.co	50.31.86.60
8881	vertex42.com	216.177.136.65
8889	streamay.com	198.12.83.146
8950	doortodoor.co.kr	61.33.235.20
8991	ecpic.com.cn	112.64.185.50
9016	transrush.com	113.106.94.46
9093	real.gr	62.1.44.131
9158	ntt.com	210.226.39.112
9242	translate.ru	62.152.52.123
9266	ddo.jp	219.94.135.204
9315	cpmfx.com	81.4.124.18
9324	femina.mk	217.16.95.60
9348	ytn.co.kr	183.111.158.30
9352	numbeo.com	176.9.57.206
9358	kotree.com	121.254.168.49
9411	iporter.com	222.239.73.34
9467	bharatiyamobile.com	72.167.40.178
9470	wileyplus.com	199.171.200.191
9480	automaticmobilecash.com	75.98.168.189
9494	bolsademulher.com	178.32.160.243

Alexa Rank	Domain	Address Tested
9502	brokenlinkcheck.com	96.43.131.30
9516	hitosara.com	125.63.40.49
9554	sd864.com	203.175.171.38
9587	dream-demo.com	198.154.224.109
9597	closermag.fr	83.231.216.103
9598	webike.net	125.206.119.33
9674	lifemedia.jp	210.131.1.196
9755	kproxy.com	76.73.41.170
9759	resona-gr.co.jp	202.211.194.111
9797	benchmark.pl	195.138.211.170
9850	183.com.cn	211.156.219.109
9919	imovelweb.com.br	152.186.33.197
9934	heydouga.com	65.39.253.110
9944	geo-online.co.jp	203.131.196.197
9978	shafaf.ir	94.182.146.19
9985	navercorp.com	125.209.210.19

The complete list of Alex Top 1 Million domains with servers that permit RSA_EXPORT cipher suites is available here (vulnerable.txt).