# Справочник по уязвимости OpenSSL Heartbleed

***Что может узнать атакующий***

Приватный ключ TLS сервера, приватный ключ TLS клиента (если клиент уязвим), cookies, логины, пароли и любые другие данные, которыми обменивается сервер и его клиенты. При этом не нужно прослушивать канал связи, достаточно послать специально сформированный пакет, и это нельзя обнаружить в логах сервера.

Уязвимость двусторонняя: если уязвимый клиент подключается к серверу злоумышленника, то злоумышленник может читать память процесса клиента. Пример уязвимых клиентов: MariaDB, wget, curl, git, nginx (в режиме прокси).

***Как протестировать уязвимость***

Веб-сервисы:
— filippo.io/Heartbleed/,
— www.ssllabs.com/ssltest/,
— rehmann.co/projects/heartbeat/,
— possible.lv/tools/hb/.
Тест для клиента: reverseheartbleed.com
Скрипт на Python: gist.github.com/sh1n0b1/10100394, gist.github.com/mitsuhiko/10130454
Скрипт на Go: github.com/titanous/heartbleeder
Статистика по сайтам: gist.github.com/dberkholz/10169691

***Какие системы подвержены уязвимости***

— Уязвимы OpenSSL 1.0.1 — 1.0.1f, 1.0.2-beta1, уязвимость исправлена в OpenSSL 1.0.1g и 1.0.2-beta2 (secadv).
— OpenVPN, в том числе и под Windows — исправлено в версии I004 (загрузка)
— Любые программы, статически слинкованные с уязвимой версией OpenSSL.
— Tor (блог).

— Debian Wheezy (stable) — исправлено в OpenSSL 1.0.1e-2+deb7u5 и 1.0.1e-2+deb7u6 (security)
— Ubuntu 12.04.4 LTS — исправлено в OpenSSL 1.0.1-4ubuntu5.12 (USN)
— CentOS 6.5 — исправлено в openssl-1.0.1e-16.el6_5.7 (centos-announce)
— Redhat 6.5 — исправлено в openssl-1.0.1e-16.el6_5.7 (solutions, errata, bugzilla)
— Fedora 19 и 20 — исправлено в openssl-1.0.1e-37 (announce)
— Gentoo — исправлено в openssl-1.0.1g (GLSA)
— Slackware 14.0 и 14.1 — исправлено в openssl-1.0.1g (slackware-security)
— OpenSUSE 12.3 и 13.1 — исправлено в openssl-1.0.1e (opensuse-security-announce)

— FreeBSD 10.0 — исправлено в 10.0-RELEASE-p1 (advisories)
— OpenBSD 5.3 и 5.4 (patch)
— NetBSD 5.0.2
— Amazon — исправлено в OpenSSL 1.0.1e-37.66 (security-bulletins)
— Android 4.1.1 — остальные версии без уязвимости.

Обычно зависят от уязвимой библиотеки и требуют перезапуска:
— Веб-серверы: Nginx, Apache, почтовые серверы: Postfix, Dovecot, Jabber и прочие IM: ejabberd,
— MySQL, если используется TLS для авторизации и он зависит от OpenSSL: в CentOS, RedHat (включая Remi), Percona Server (blog).

### *Что не подвержено уязвимости*

— Windows (нет OpenSSL), MacOS (старая версия OpenSSL), Firefox, Thunderbird (по умолчанию использует NSS), Chrome/Chromium (по умолчанию использует NSS), Android (отключен heartbeat).
— Корневые и промежуточные сертификаты, которыми подписаны ключи TLS сервера (приватные ключи от них отсутствуют на сервере)
— OpenSSH (использует OpenSSL только для генерации ключей)
— OpenVPN, если использует статические ключи (не x509) или если использует в конфиге ключ вида «tls-auth ta.key 1»
— Метод распространения обновлений Unix-like ОС (чаще всего используется GnuPG для подписи).

### Как обновить систему

#### Debian, Ubuntu

```
# aptitude update
# aptitude -VR full-upgrade
```

После этого полностью перезапустить сервисы, которые используют TLS. Установщик обновления предложит перезапустить автоматически, или можно вручную:

```
# service nginx restart
# service apache2 restart
```

Полный список сервисов, которые нуждаются в перезапуске и могут быть уязвимы:

```
# lsof -n | grep -iE 'del.*(libssl\.so|libcrypto\.so)'
или
# checkrestart
```

Если не уверены, лучше полностью перезагрузить сервер.

Проверка версии:

```
# dpkg -l | grep -i openssl
# aptitude changelog openssl
```

**CentOS, RedHat, Fedora**

```
# yum update
```

После этого полностью перезапустить сервисы, которые используют TLS, например:

```
# service nginx restart
# service httpd restart
```

Полный список сервисов, которые нуждаются в перезапуске и могут быть уязвимы:

```
# lsof -n | grep -iE 'del.*(libssl\.so|libcrypto\.so)'
или
# needs-restarting
```

Если не уверены, лучше полностью перезагрузить сервер.

Проверка версии:

```
# yum list openssl
# rpm -q --changelog openssl
```

**FreeBSD**

```
# freebsd-update fetch
# freebsd-update install
```

После этого полностью перезапустить сервисы, которые используют TLS, например:

```
# service nginx restart
# service apache22 restart
```

Если не уверены, лучше полностью перезагрузить сервер.
Проверка версии:

```
# freebsd-version
```

### *Отзыв TLS ключей и смена паролей*

— Если атакующий смог собрать полностью приватный ключ, то он может использовать его для создания поддельного сайта, или для расшифровки подслушанных сессий. Поэтому рекомендуется отозвать сертификаты, ключи от которых могли попасть к атакующему.

— Если браузер клиентов передавал пароли на сайт без hash+salt, а в чистом виде, то эти пароли также могут быть скомпрометированы.

### На будущее

— Нужно убедиться, что браузер проверяет, не отозван ли сертификат сайта, который он посещает.
Firefox по умолчанию проверяет OSCP, а последние версии также поддерживают OCSP Stapling; Safari проверяет по умолчанию с версии Mac OS X 10.7 (Lion); Chrome не проверяет по умолчанию (в настройках раздел HTTPS/SSL), OCSP Stapling не поддерживается; Internet Explorer по умолчанию проверяет OSCP, но не поддерживает OCSP Stapling; Opera проверяет OSCP по умолчанию; Safari не проверяет OSCP по умолчанию. Настройки разных браузеров.

— На сервере желательно включить Perfect forward secrecy (PFS). При этом даже при компрометации приватного ключа злоумышленник не сможет расшифровать прошлый или будущий подслушанный трафик. Для этого нужно включить Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) или Diffie-Hellman Ephemeral (DHE). Настройка сервера, тестирование.