Уязвимости Copy Fail, Dirty Frag, Fragnesia и свежие баги в Exim/nginx: что проверить на облачном сервере

За последнее время в публичном поле появилось несколько заметных уязвимостей в инфраструктурных компонентах: **Copy Fail**, **Dirty Frag**, **Fragnesia**, а также уязвимости в **Exim** и **nginx**.

Часть таких уязвимостей относится к локальному повышению привилегий: в уязвимой конфигурации непривилегированный пользователь или процесс может получить больше прав в системе, вплоть до root.

Другие могут затрагивать почтовые и веб-сервисы — в зависимости от того, какое ПО установлено на сервере и как оно настроено.

На стороне платформенной инфраструктуры Timeweb Cloud мы проверили затронутые компоненты и применили необходимые меры защиты.

Если вы используете облачный сервер и самостоятельно администрируете операционную систему, рекомендуем проверить и обновить компоненты внутри вашей ВМ.

Быстрый чек-лист:

1. Сделайте резервную копию или снапшот сервера.
2. Обновите системные пакеты и ядро ОС.
3. Перезагрузите сервер после обновления ядра.
4. Обновите Exim, если он установлен и используется.
5. Обновите nginx, если он установлен.
6. Проверьте пользователей с sudo/wheel-доступом.
7. Проверьте актуальность SSH-ключей.

Сделайте снапшот или резервную копию

https://timeweb.cloud/docs/cloud-servers/manage-servers/backup

Перед обновлением ядра и системных пакетов рекомендуем сделать снапшот сервера или актуальную резервную копию.

Это позволит быстро восстановиться, если после обновления возникнут проблемы совместимости с приложением, драйверами, сетевыми настройками или сторонними модулями.

Обновите ядро и системные пакеты

Уязвимости уровня ядра обычно исправляются через обновления дистрибутива. Поэтому основной способ защиты — установить актуальные обновления безопасности из официальных репозиториев вашей ОС.

Debian / Ubuntu

sudo apt update
sudo apt upgrade -y

Если используется стандартное ядро дистрибутива, также проверьте, что установлен актуальный метапакет ядра.

Для Ubuntu:

sudo apt install --only-upgrade linux-generic -y

Для Debian:

sudo apt install --only-upgrade linux-image-amd64 -y

После обновления ядра перезагрузите сервер:

sudo reboot

Проверить текущую версию ядра:

uname -r

AlmaLinux / Rocky Linux / RHEL / Fedora

sudo dnf upgrade --refresh -y

После обновления ядра перезагрузите сервер:

sudo reboot

Проверить текущую версию ядра:

uname -r

openSUSE

sudo zypper refresh
sudo zypper update -y

После обновления ядра перезагрузите сервер:

sudo reboot

Проверить текущую версию ядра:

uname -r

Arch Linux

sudo pacman -Syu

После обновления ядра перезагрузите сервер:

sudo reboot

Проверить текущую версию ядра:

uname -r

Обновите Exim, если он используется

Если на сервере установлен и используется Exim, обновите его до актуальной версии из репозиториев вашего дистрибутива.

Проверить версию Exim:

exim --version

Debian / Ubuntu

sudo apt update
sudo apt install --only-upgrade exim4 -y

Перезапустить сервис:

sudo systemctl restart exim4

Проверить статус:

sudo systemctl status exim4

AlmaLinux / Rocky Linux / RHEL / Fedora

sudo dnf upgrade exim -y

Перезапустить сервис:

sudo systemctl restart exim

Проверить статус:

sudo systemctl status exim

Если Exim не установлен или не используется, дополнительных действий по этому пункту не требуется.

Обновите nginx, если он используется

Если на сервере установлен nginx — например, как веб-сервер, reverse proxy или frontend перед приложением — обновите его до актуальной версии из репозиториев вашей ОС или из официального репозитория nginx, если вы используете его.

Проверить версию nginx:

nginx -v

Debian / Ubuntu

sudo apt update
sudo apt install --only-upgrade nginx -y

Проверить конфигурацию:

sudo nginx -t

Применить изменения:

sudo systemctl reload nginx

Если reload не сработал, используйте restart:

sudo systemctl restart nginx

AlmaLinux / Rocky Linux / RHEL / Fedora

sudo dnf upgrade nginx -y

Проверить конфигурацию:

sudo nginx -t

Применить изменения:

sudo systemctl reload nginx

Если reload не сработал:

sudo systemctl restart nginx

Если nginx не установлен или не используется, дополнительных действий по этому пункту не требуется.

Проверьте пользователей с административными правами

После обновлений стоит проверить, у кого есть доступ к повышенным привилегиям.

Debian / Ubuntu

Проверить пользователей в группе sudo:

getent group sudo

AlmaLinux / Rocky Linux / RHEL / Fedora

Проверить пользователей в группе wheel:

getent group wheel

Удалите административные права у пользователей, которым они больше не нужны.

Проверьте SSH-ключи

Проверьте, какие SSH-ключи имеют доступ к серверу.

Для текущего пользователя:

cat ~/.ssh/authorized_keys

Для других пользователей проверьте файлы:

/home/<user>/.ssh/authorized_keys

Удалите ключи бывших сотрудников, подрядчиков, временных пользователей и всех, кому доступ больше не нужен.

Проверьте настройки SSH

Если на сервере до сих пор разрешен вход по паролю, рекомендуем отключить его и использовать авторизацию по SSH-ключам.

Откройте конфигурацию SSH:

sudo nano /etc/ssh/sshd_config

Рекомендуемые параметры:

PasswordAuthentication no
PermitRootLogin prohibit-password

Перед применением убедитесь, что у вас есть рабочий SSH-ключ и вы не потеряете доступ к серверу.

Проверить конфигурацию SSH:

sudo sshd -t

Перезапустить SSH:

sudo systemctl restart sshd

На некоторых дистрибутивах сервис может называться ssh :

sudo systemctl restart ssh

Временные меры защиты

Основная рекомендация — установить обновления безопасности из репозиториев вашего дистрибутива.

Временные обходные меры, например блокировка отдельных модулей ядра, стоит применять только если:

• для вашей ОС ещё нет исправления;
• вы понимаете, какие компоненты отключаете;
• вы проверили, что это не нарушит работу ваших сервисов;
• рекомендация подтверждена advisory вашего дистрибутива или вашей технической командой.

Некоторые обходные меры могут повлиять на работу сетевых функций, IPsec или другого ПО. Поэтому не применяйте такие команды без проверки совместимости с вашей конфигурацией.