Компенсирующие меры по уязвимости kernel-lt CVE-2026-31431

Окружение

- **Версия РЕД ВИРТ:** 7.3

Для предотвращения эксплуатации уязвимости kernel-lt CVE-2026-31431 на хостах и менеджере РЕД ВИРТ предусмотрены следующие компенсирующие меры:

Для хостов:

1. Хост нужно перевести в режим обслуживания через веб-интерфейс РЕД ВИРТ.
2. В терминале хоста необходимо произвести установку пакетов
   - для РЕД ВИРТ 7.3, работающей на 5 ядре:

     ```
     dnf install kernel-lt-5.15.167-20.el7virt.x86_64
     ```

   - для РЕД ВИРТ 7.3, работающей на 6 ядре:

     ```
     dnf install kernel-lt-6.1.143-6.el7virt.x86_64
     ```

3. Произвести перезагрузку системы хоста:

   ```
   reboot
   ```

   Убедиться, что хост загружен на верной версии ядра:

   ```
   uname -a
   ```

4. Выполнить проверочный скрипт (вводится одной командой в терминал хоста):

   ```
   python3 -c 'import socket;s=socket.socket(38,5,0);s.bind(("aead","authencesn(hmac(sha256),cbc(aes))"));print("vulnerable");s.close()'
   2>/dev/null || echo "Not vulnerable / blocked"
   ```

5. Если выполнение скрипта закончилось выводом "**vulnerable**", то:
   - Выполнить команду удаления модуля ядра:

     ```
     rmmod algif_aead
     ```

   - Произвести предотвращение выгрузки, выполнив команды:

     ```
     sudo tee /etc/modprobe.d/disable-algif-aead.conf > /dev/null <<'EOF'
     ```

     ```
     install algif_aead /bin/false
     ```

     ```
     EOF
     ```

   - Произвести перезагрузку системы, выполнив команду:

     ```
     reboot
     ```

6. Выполнить команду из шага (4):

   ```
   python3 -c 'import socket;s=socket.socket(38,5,0);s.bind(("aead","authencesn(hmac(sha256),cbc(aes))"));print("vulnerable");s.close()'
   2>/dev/null || echo "Not vulnerable / blocked"
   ```

Результат выполнения команды должен вернуть значение "**Not vulnerable / blocked**".

Для ВМ HostedEngine:

1. В терминале хоста, где запущена ВМ HostedEngine, выполнить команду включения режима глобального обслуживания:

   ```
   hosted-engine --set-maintenance --mode=global
   ```

2. С помощью команды на этом же хосте:

   ```
   hosted-engine --vm-status
   ```

Убедиться, что в выводе присутствует запись:

```
!! Cluster is in GLOBAL MAINTENANCE mode !!
```

3. Далее необходимо перейти в терминал ВМ HostedEngine и произвести установку пакетов
   - для РЕД ВИРТ 7.3, работающей на 5 ядре:

     ```
     dnf install kernel-lt-5.15.167-20.el7virt.x86_64
     ```

   - для РЕД ВИРТ 7.3, работающей на 6 ядре:

     ```
     dnf install kernel-lt-6.1.143-6.el7virt.x86_64
     ```

4. Произвести перезагрузку системы ВМ HostedEngie:

   ```
   reboot
   ```

   Проверить статус ВМ HostedEngine, выполнив в терминале хоста, где была запущена эта ВМ:

   ```
   hosted-engine --vm-status
   ```

   Если ВМ HostedEngine не запускается, то выполнить команду на хосте:

   ```
   hosted-engine --vm-start
   ```

5. Необходимо убедиться, что ВМ HostedEngine загружена на верной версии ядра. Для этого в терминале ВМ выполнить команду:

   ```
   uname -a
   ```

6. Выполнить проверочный скрипт (вводится одной командой в терминал ВМ HostedEngine):

   ```
   python3 -c 'import socket;s=socket.socket(38,5,0);s.bind(("aead","authencesn(hmac(sha256),cbc(aes))"));print("vulnerable");s.close()'
   2>/dev/null || echo "Not vulnerable / blocked"
   ```

7. Если выполнение скрипта закончилось выводом "**vulnerable**", то:
   - Выполнить команду удаления модуля ядра:

     ```
     rmmod algif_aead
     ```

   - Произвести предотвращение выгрузки, выполнив команды:

     ```
     sudo tee /etc/modprobe.d/disable-algif-aead.conf > /dev/null <<'EOF'
     ```

     ```
     install algif_aead /bin/false
     ```

     ```
     EOF
     ```

   - Произвести перезагрузку системы ВМ HostedEngine, как описано в шаге (4).

8. Выполнить команду в терминале ВМ HostedEngine из шага (6):

   ```
   python3 -c 'import socket;s=socket.socket(38,5,0);s.bind(("aead","authencesn(hmac(sha256),cbc(aes))"));print("vulnerable");s.close()'
   2>/dev/null || echo "Not vulnerable / blocked"
   ```

Результат выполнения команды должен вернуть значение "**Not vulnerable / blocked**".

Источник: https://redvirt.red-soft.ru/base/knowledge-base/kernel-lt-cve-2026-31431/