Меры по защите информации в операционной системе Linux

1. Уязвимость ядра операционной системы Linux (версия от 5.8 до 5.16.11, от 5.8 до 5.15.25 и от 5.8 до 5.10.102) (BDU:2022-01166, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – высокий), позволяющая авторизованному нарушителю (непривилегированному пользователю) выполнить произвольный код с привилегиями root. В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;

обеспечить принудительную смену паролей пользователей;

ограничить удаленный доступ к операционной системе (SSH и другие протоколы);

ограничить доступ к командной строке для недоверенных пользователей; использовать антивирусные средства защиты;

осуществлять мониторинг действий пользователей;

использовать системы управления доступом (таких, как SELinux, AppArmor идругие системы управления доступом).

1.1. Обеспечить аутентификацию по SSH-ключам, а также отключить возможность входа с правами «root» (повышение привилегий должно происходить посредством настройки политик sudo). Отключить прямой доступ по SSH из сети «Интернет».

1.2. Включить службу логирования auditd, а также осуществлять централизованный сбор и мониторинг событий, как минимум на выполнение команд: «sudo-l», «export HISTFILE=/dev/null», «unset HISTFILE», history –cw и тд., а также auth.log.

1.3. Осуществлять мониторинг выполнения команд для служебных (сервисных) учетных записей не типичных для служб, к которым они относятся.

1.4. Осуществлять сбор и мониторинг событий создания SSH-тоннелей и проброса портов.

1.5. Осуществлять сбор и мониторинг событий изменения файлов /etc/passwd, /ect/shadow.

1.6. Производить проверку контрольных сумм (md5/sha512) загружаемых и устанавливаемых файлов.

2. Уязвимость отечественной операционной системы (Astra Linux, Special Edition, Astra Linux Common Edition, РЕД ОС, Альт 8 СП, Синтез М), применяемые в информационных системах органов государственной власти и организации Российской Федерации.

В целях предотвращения эксплуатации указанной уязвимости рекомендуем установить следующие обновления для указанных операционных систем:

для РЕД ОС: http://repo.red-soft.ru/redos/7.3/x86_64/updates/; для Альт 8 СП: https://altsp.su/obnovleniya-bezopasnosti/

для Astra Linux:

https://wiki.astralinux.ru/astra-linux-se17-bulletin-2022-0318SE17MD; https://wiki.astralinux.ru/astra-linux-ce212-MD-2022-0318MD; https://wiki.astralinux.ru/astra-linux-se17-bulletin-2022-0318SE17MD; https://wiki.astralinux.ru/astra-linux-se47-bulletin-2022-0318SE47MD; https://wiki.astralinux.ru/astra-linux-se16-bulletin-20220318SE16MD; https://wiki.astralinux.ru/astra-linux-ce212-MD-2022-0318MD.

для Альт 8 СП: обновление программного обеспечения до актуальной версии; для Синтез М: обновление программного обеспечения до версии 20220314-1820 и выше.

3. Уязвимость компонента tc_new_tfilter ядра Linux (BDU:2022-01644, уровень опасности по CVSS 2.0 – средний, по CVSS 3.0 – средний), связанная с возможностью использования памяти после освобождения. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

-отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;

-обеспечить принудительную смену паролей пользователей;

-ограничить удаленный доступ к операционной системе (SSH и другие протоколы);

-ограничить доступ к командной строке для недоверенных пользователей; использовать системы управления доступом (SELinux, AppArmor и другие системы).

4. Уязвимость библиотеки gzip (BDU:2022-02113, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с ошибками при обработке имен файлов. Эксплуатация данной уязвимости может позволить нарушителю, действующему удаленно, записать произвольные файлы в систему с помощью утилит командной строки zgrep и xzgrep.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

- ограничить доступ недоверенных пользователей к терминалу Linux;
- использовать замкнутую программную среду.

5. Уязвимость функции xs_xprt_free системы удаленного вызова процедур Sun RPC (Open Network Computing Remote Procedure Call) ядра операционных систем Linux (BDU:2022-02112, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий), связанная с ошибками управления состоянием. Эксплуатация данной уязвимости может позволить нарушителю вызвать отказ в обслуживании.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо отключить сервис sunrpc.

6. Уязвимость функции nft_expr_init программного обеспечения фильтрации пакетов Netfilter ядра операционной системы Linux связана с возможностью использования памяти после освобождения (BDU:2022-03283, уровень опасности по CVSS 2.0 – высокий, по CVSS 3.0 – высокий). Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо:

-отключение неиспользуемых учетных записей, а также учетных записей недоверенных пользователей;

-ограничение доступа к командной строке для недоверенных пользователей;

-использование антивирусных средств защиты;

-мониторинг действий пользователей;

-использование входных данных только из доверительных источников;

-использование систем управления доступом.

7. Уязвимость функции nft_set_desc_concat_parse() ядра Linux (BDU:2022-04090, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании или выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо принять следующие меры:

-отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;

-ограничить доступ к командной строке для недоверенных пользователей;

-использовать антивирусные средства защиты;

-осуществлять мониторинг действий пользователей;

-использовать системы управления доступом (такие, как SELinux, AppArmor и другие системы управления доступа).

8. Устранения уязвимости функции pxa3xx_gcu_write (drivers/video/fbdev/pxa3xx-gcu.c) ядра операционной системы Linux (BDU:2022-05539, уровень опасности по CVSS 2.0 – критический, по CVSS 3.0 – критический), вызванной целочисленным переполнением. Эксплуатация данной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В случае невозможности установки обновления ПО необходимо принять следующие меры:

- отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;
- принудительно сменить пароли пользователей;
- ограничить удаленный доступ к операционной системе недоверенных пользователей (например, SSH, RDP и другие протоколы удаленного доступа);
- ограничить доступ к командной строке для недоверенных пользователей;
- использовать антивирусные средства защиты информации;
- осуществить мониторинг действий пользователей;
- использовать системы управления доступом (такие, как SELinux, AppArmor и другие системы).

9. Устранения уязвимости интерфейса асинхронного ввода/вывода io_uring ядра операционной системы Linux (BDU:2022-06407, уровень опасности по CVSS 2.0 - высокий уровень опасности, по CVSS 3.0 - критический уровень опасности), связанной с возможностью использования памяти после освобождения. Эксплуатация указанной уязвимости может позволить нарушителю повысить свои привилегии. В случае невозможности установки обновления программного обеспечения необходимо принять следующие меры:

-отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;

ограничить доступ к командной строке для недоверенных пользователей;

использовать антивирусные средства защиты; производить мониторинг действий пользователей.

10 Уязвимость функции cfg80211_update_notlisted_nontrans файла net/wireless/scan.c ядра операционных систем Linux (BDU.2022-06272, уровень опасности по CVSS 2.0 — высокий уровень опасности, по CVSS 3.0 — высокий уровень опасности), связанная с переполнением буфера. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

11. Уязвимость функционала подсчета ссылок в режиме BSS (Basic Service

Set) ядра операционных систем Linux (BDU.2022-06273, уровень опасности по CVSS 2.0 — высокий уровень опасности, по CVSS 3.0 — высокий уровень опасности), связанная с возможностью использования памяти после освобождения. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

12.Уязвимость ядра операционных систем Linux (BDU:2022-06274, уровень опасности по CVSS 2.0 — высокий уровень опасности, по CVSS 3.0 — высокий уровень опасности), связанная с возможностью использования памяти после освобождения в коде разбора MBSSID. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

-ограничить использование WLAN-сетей;

-ограничить подключение к сетям связи общего пользования «Интернет».

13. Уязвимость компонента StringSubstitutor библиотеки Apach Common Text (BDU:2022-06275, уровень опасности по CVSS 2.0 — критический уровень опасности, по CVSS 3.0 — критический уровень опасности), связанная с неверным управлением генерацией кода. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

-использовать межсетевые экраны уровня веб-приложений (WAF);

-изменить метод InetAddress::checkNumericZone для удаления итерации проверки символов «[» и «]».

14. Уязвимость функций net/bluetooth/12cap_core.c, 12cap_connect и 12cap_le_connect_req ядра операционных систем Linux (BDU:2022-07074, уровень опасности по CVSS 2.0 – высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), связанной с возможностью использования памяти после освобождения. Эксплуатация указанной уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 года (прилагается).

В случае невозможности установки обновления программного обеспечения необходимо принять следующие компенсирующие меры:

-ограничить использование WLAN-сетей;

-ограничить возможность подключения к общедоступной сети (Интернет).

15. Уязвимость функции must_mkdir_and_open_with_perms() утилиты snap-confine операционной системы Ubuntu (BDU:2022-07107, уровень опасности по CVSS 2.0 – высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), связанная с ошибками синхронизации при использовании общего ресурса. Эксплуатация данной уязвимости может позволить нарушителю повысить свои привилегии или выполнить произвольный код.

Если установка обновления программного невозможна необходимо принять следующие компенсирующие меры:

-отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей;

-принудительной сменить пароли пользователей;

-ограничить доступ к командной строке для недоверенных пользователей;

-использовать антивирусные средства защиты;

-производить мониторинг действий пользователя.