Меры по повышению защищенности информационной инфраструктуры Российской Федерации

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками при реализации компьютерных атак на информационную инфраструктуру Российской Федерации активно эксплуатируются уязвимости программного обеспечения.

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, просим обратить внимание на необходимость устранения уязвимости функции sudoedit программы системного администрирования Sudo операционных систем семейства Linux (BDU:2023-00210, уровень опасности по CVSS 3.0 — высокий уровень опасности), связанной с ошибками при обработке дополнительных аргументов в переменных среды. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии.

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 г. (fstec.ru/tekhnicheskaya- zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

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

ограничить использование sudoedit путем добавления в файл sudoers следующей строки;

Defaults!sudoedit env_delete+="SUDO_EDITOR VISUAL EDITOR";

использовать Cmnd_Alias для ограничения возможности редактирования определенных файлов

Cmnd_Alias EDIT_MOTD = sudoedit /etc/motd

Defaults!EDIT_MOTD env_delete+="SUDO_EDITOR VISUAL EDITOR"

user ALL = EDIT_MOTD;

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

осуществить принудительную смену паролей пользователей;

ограничить удаленный доступ к операционной системе недоверенных пользователей;

ограничить доступ к командной строке для недоверенных пользователей;

осуществлять мониторинг действий пользователей.

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, просим обратить внимание на необходимость устранения следующих уязвимостей:

1. Уязвимость метода сборки кода utils.exec прокси-менеджера

управления хостами Nginx Proxy Manager (BDU:2023-00349, уровень опасности по CVSS 3.0 — высокий), которая существует из-за непринятия мер по нейтрализации специальных элементов, используемых в команде операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнять произвольные команды на сервере.

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 г. (fstec.ru/tekhnicheskaya- zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

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

использовать средства межсетевого экранирования уровня веб-приложений;

использовать антивирусное программное обеспечение;

использовать сторонние средства контроля доступа пользователей к программному продукту из общедоступных сетей (Интернет).

2. Уязвимость программного пакета Cisco Industrial Network Director (BDU:2023-00350, уровень опасности по CVSS 3.0 — высокий), связанная с возможностью получения доступа к статическому секретному ключу. Эксплуатация уязвимости может позволить нарушителю получить доступ ко всем контролируемым системам.

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 г. (fstec.ru/tekhnicheskaya- zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

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

минимизировать пользовательские привилегий;

осуществлять мониторинг действий пользователей;

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

осуществить принудительную смену паролей пользователей.

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, просим обратить внимание на необходимость устранения следующих уязвимостей:

1. Уязвимость реализации протокола Windows Point-to-Point Tunneling Protocol операционной системы Windows (BDU:2023-00438, уровень опасности по CVSS 3.0 - высокий), связанная с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю,

действующему удалённо, 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 г. (fstec.ru/tekhnicheskaya- zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

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

использовать средства межсетевого экранирования для ограничения доступа к серверу RAS;

применять системы обнаружения и предотвращения вторжений.

2. Уязвимость демона обработки потоков flowd операционных систем Juniper Networks Junos OS маршрутизаторов серии SRX (BDU:2023-00488, уровень опасности по CVSS 3.0 - высокий), связанная с ошибками освобождения памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.

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 г. (fstec.ru/tekhnicheskaya- zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

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

использовать средства межсетевого экранирования для ограничения удалённого доступа к устройству;

отключить процесс iked, осуществив проверку статуса отключения процесса с помощью команды:

show system processes extensive | match "KMD|IKED".

По имеющейся в ФСТЭК России информации, злоумышленниками активно используются уязвимости в сайтах государственных органов (организаций), связанные с открытой переадресацией (тип ошибки CWE-601), а также с недостаточной защитой структуры веб-страницы («межсайтовый скриптинг» или «XSS», тип ошибки CWE-79) в целях размещения в них рекламы противоправных информационных ресурсов.

Наличие указанных уязвимостей на официальных сайтах государственных органов создает предпосылки к реализации угроз безопасности информации, в том числе к нарушению их функционирования, а также изменению содержимого, размещаемого на них.

В целях предотвращения реализации указанных уязвимостей считаем необходимым принять следующие дополнительные меры по защите информации:

осуществить проверку на предмет наличия уязвимостей

на официальных сайтах, связанных с ошибками типов CWE-601, CWE-79, в том числе с применением инструментов анализа веб-приложений;

в случае обнаружения указанных уязвимостей внести изменения в программный код веб-приложения (например, добавление проверок ресурса, на который осуществляется переадресация, очистка пользовательского ввода);

использовать политику защиты содержимого (Content Security Policy);

ограничить функцию открытой переадресации на внешние веб-сайты по «белому списку».

С целью предотвращения реализации угроз безопасности информации. Связанных с эксплуатацией уязвимостей, просим обратить внимание на необходимость устранения следующих уязвимостей:

1. Уязвимость программной платформы Cisco Iox (BDU:2023-00549, уровень опасности по CVSS 3.0 — высокий), связанная с недостаточной проверкой входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнять произвольные команды в операционной системе с привилегиями root - пользователя.

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 г. (fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye- dokumenty).

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

отключить функцию Cisco IOx путём ввода команды:

по iox;

выполнить проверку программного средства на подверженность уязвимости осуществляется путём ввода следующей команды:

show iox;

Пример вывода для неуязвимого программно-аппаратного средства (оборудование не подвержено уязвимости, если оно поддерживает собственный Docker и включено Dockerd):

IOx Infrastructure Summary:

IOx service (CAF) : Running
IOx service (HA) : Running
IOx service (lOxman) : Running
lOx service (Sec storage) : Running
Libvirtd 5.5.0 : Running
Dockerd v19.03.13-ce : Running
Sync Status : Disabled

2. Уязвимость гипервизора VMware Workstation (BDU:2023-00571, уровень опасности по CVSS 3.0 — высокий), связанная с ошибками

разграничения доступа. Эксплуатация уязвимости может позволить нарушителю удалить произвольные файлы в корневой операционной системе.

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 г. (fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye- dokumenty).

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

отключить неиспользуемые учетные записи, а также учетные записи недоверенных пользователей корневой операционной системы;

осуществить минимизацию пользовательских привилегий.

3. Уязвимость компонента Upload программного средства для работы с веб-приложениями Oracle Web Applications Desktop Integrator (BDU:2023-00572, уровень опасности по CVSS 3.0 — критический), связанная с ошибками при обработке входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить полный контроль над приложением.

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 г. (fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty).

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

использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности удаленного доступа.