Приложение

СВЕДЕНИЯ
о выявленных уязвимостях программного обеспечения, мерах противодействия и компенсирующих мерах защиты информации

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

1. Уязвимость функции SetVirtualServerSettings микропрограммного обеспечения маршрутизаторов D-Link DIR-867 (BDU:2023-01391, уровень опасности по CVSS 3.0 — критический), связанная с возможностью внедрения команд. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольные команды в операционной системе устройства от имени root-пользователя путем манипулирования значением параметра LocallPAddress.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также 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 и средства обнаружения и предотвращения вторжений для отслеживания подключений к устройству;

ограничить доступ к веб-интерфейсу устройства из внешних сетей;

использовать средства межсетевого экранирования с целью ограничения доступа к устройству.

2. Уязвимость компонента Passwords браузера Google Chrome (BDU:2023-01469, уровень опасности по CVSS 3.0 — критический), связанная с использованием памяти после её освобождения. 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 тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также 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 антивирусной защиты с функцией контроля доступа к веб-ресурсам;

осуществить контролируемый доступ в сеть Интернет посредством регламентации разрешенных сетевых ресурсов и соединений;

реализовать запуск веб-браузера от имени пользователя с минимальными возможными привилегиями в операционной системе;

использовать альтернативные веб-браузеры;

применять системы обнаружения и предотвращения вторжений.

3. Уязвимость терминального сервера NPort 6000 и диспетчера драйверов NPort Windows Driver Manager (BDU:2023-01295, уровень опасности по CVSS 3.0 — критический), связанная с ошибками процедуры подтверждения подлинности сертификата. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить атаку типа «человек посередине».

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также Методикой оценки уровня критичности программных, программно-аппаратных средств, утвержденной ФСТЭК России от 28 октября 2022 г. (fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/l 14-spetsialnye-normativnye-dokumenty).

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

использовать физическое или логическое разграничение доступа к вычислительной сети с терминальным сервером Moxa NPort путем разграничения межсетевыми экранами с выделением отдельной подсети;

ограничить возможность удаленного доступа из внешних сетей;

использовать виртуальные частные сети для организации удаленного доступа.

4. Уязвимость механизма обработки и фрагментации пакетов туннельного протокола в операционной системе Cisco IOS XE (BDU:2023-01490, уровень опасности по CVSS 3.0 — высокий), связанная с ошибками при обработке входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании.

В целях предотвращения возможности эксплуатации указанной уязвимости рекомендуется установить обновление программного обеспечения в соответствии с Методикой тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также 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:

осуществить отключение туннельного протокола;

для проверки активности туннельного протокола необходимо ввести следующую команду:

show ip interface brief | count Tun

Number of lines which match regexp = 1

в случае, если параметр regexp = 0 - туннельные интерфейсы не настроены, если regexp = 1 - настроены;

использовать средств межсетевого экранирования для ограничения возможности отправки специально сформированных пакетов на устройства под управлением Cisco IOS XE.

5. Уязвимость исполняемого файла iplogging.cgi микропрограммного обеспечения ALEOS маршрутизаторов Sierra Wireless (BDU:2023-01491, уровень опасности по CVSS 3.0 — высокий), существующая из-за непринятия мер по нейтрализации специальных элементов, используемых в команде операционной системы. Эксплуатация 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 тестирования обновлений безопасности программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., а также 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 доступ к ACEManager из внешних сетей;

использовать Sierra Wireless Airlink Management System (ALMS) или альтернативную платформу управления устройствами для удаленного управления устройствами ALEOS;

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