РЕЗОЛЮЦИЯ

Исполняющего обязанности начальника
Управления культуры

4545091, г.Челябинск, ул. Цвиллинга, 7
тел.7007442, 2633921, факс 2636566

Иванову А. В.

« 15 » 02 2022 Е. В. Войтюк

вх. № 642 от 15.02 2022

ИОННЫХ ТЕХНОЛОГИЙ, СВЯЗИ
Я ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Челябинск, 454080, Россия
3-53, E-mail: info@mininform74.ru
5.1310939/745301001, ОКПО 68647084

Главам городских округов и
муниципальных районов
Челябинской области

оссии информации злоумышленниками
в сайтах государственных органов
ереадресацией (тип ошибки CWE-601), а
руктуры веб-страницы («межсайтовый
CWE-79) в целях размещения в них
нных 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 необходимо 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».

Также 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 органов местного самоуправления активно эксплуатируются уязвимости программного обеспечения.

Управление культуры
Администрации города Челябинска
Вх. № 642
« 15 » 02 2023 г.

Администрация г. Челябинска
Заместитель Главы Администрации
города по социальному развитию
Вх. 493
« 13 » 02 2023

5 1885/2300
09.02.2023

МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, СВЯЗИ И ЦИФРОВОГО РАЗВИТИЯ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

Ул. Сони Кривой, д. 75а, Челябинск, 454080, Россия
телефон/факс: (351) 232-33-53, E-mail: info@mininform74.ru
ОГРН 1107451016860, ИНН/КПП 7451310939/745301001, ОКПО 68647084

09.02.2023 № 1602/688

на №_____от_____

Главам городских округов и муниципальных районов Челябинской области

По имеющейся во 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 необходимо 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».

Также 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 органов местного самоуправления активно эксплуатируются уязвимости программного обеспечения.

Управление культуры Администрации города Челябинска
Вх. № 692
«15» 02 2023 г.

Администрация г. Челябинска
Заместитель Главы Администрации города по социальному развитию
Вх. 493
«13» 02 2023

5 1885/2302
09.02.2023

С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, обращаю внимание на необходимость устранения следующих уязвимостей.

1. Уязвимость веб-интерфейса контроллера доставки приложений FortiADC (BDU:2023-00040, уровень опасности по CVSS 2.0 – высокий уровень опасности, по CVSS 3.0 – высокий уровень опасности), связанная с непринятием мер по нейтрализации специальных элементов, используемых в команде операционной системы. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнять произвольные команды путем отправки специально сформированных HTTP-запросов.

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

использовать средства межсетевого экранирования уровня веб-приложений;

отключить неиспользуемые учетные записи;

применять системы обнаружения и предотвращения вторжений;

ограничить доступ к программному средству из общедоступных сетей.

2. 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 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).

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

минимизировать пользовательские привилегии;

осуществлять мониторинг действий пользователей;

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

осуществить принудительную смену паролей пользователей.

4. 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 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.

5. Уязвимость домена 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 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".

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

Актуальные сведения об угрозах безопасности информации и уязвимостях системного и прикладного программного обеспечения систематически обновляются в Банке данных угроз безопасности информации, ведение которого осуществляет ФСТЭК России (bdu.fstec.ru).

Для использования в работе высылаю информационную справку о результатах мониторинга сведений о критических уязвимостях программного обеспечения объектов информационной инфраструктуры, проводимого Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (Приложение).

Прошу довести указанную информацию до ответственных сотрудников, подведомственных организаций и реализовать меры, направленные на нейтрализацию угроз безопасности информации, связанных с эксплуатацией уязвимостей.

Прошу обратить внимание, что публикация указанных мер защиты информации в сети «Интернет» и средствах массовой информации не допускается.

Кроме того сообщаю, что ФСТЭК России 25 ноября 2022 г. разработаны и утверждены Рекомендации по обеспечению безопасной настройки операционных систем Linux. Рекомендации размещены на официальном сайте ФСТЭК России (www.fstec.ru) в разделе «Документы/Информационные и аналитические материалы».

При возникновении вопросов по материалам письма прошу обращаться:

Управление ФСТЭК по УрФО: (343) 372-18-62 – Киршин Николай Аркадьевич; (343) 372-18-52 – Заверячев Михаил Сергеевич.

Приложение: в электронном виде.

Исполняющий обязанности Министра В.В. Кокорюкин

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 308417805194074188514908136926111759160448543081

Владелец: Кокорюкин Василий Владимирович

Действителен с 02.12.2021 по 02.03.2023

Тепис 5-527/23

Лихачева Алиса Александровна
(351) 263-64-36

4

Приложение

Информационная справка
о результатах мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, проводимого федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»

Идентификатор и описание	Возможные меры защиты
BDU:2023-00346 **CVE-2022-22274** Уязвимость веб-интерфейса управления операционной системы SonicOS связана с возможностью переполнения буфера в стеке. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: использование средств межсетевого экранирования уровня веб-приложений; использование механизма «белых» списков для предоставления доступа к веб-интерфейсу управления только с доверенных IP-адресов; ограничение доступа к межсетевому экрану из внешних сетей (Интернет); использование VPN для организации удаленного доступа. Источники информации: https://nvd.nist.gov/vuln/detail/CVE-2022-22274 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003
BDU:2023-00347 **CVE-2022-46823** Уязвимость реализации модуля единого входа в приложения (SAML) программной платформы развертывания и проверки программных приложений Mendix связана с недостаточной защитой структуры веб-страницы. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к защищаемой информации	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.3) CVSS v3:AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N Компенсирующие меры: включение механизма двухфакторной аутентификации; использование средств межсетевого экранирования; использование сторонних средств контроля доступа пользователей (VPN и др.) к программному продукту из общедоступных сетей (Интернет); использование систем обнаружения и предотвращения вторжений. Источники информации: https://cert-portal.siemens.com/productcert/pdf/ssa-496604.pdf https://nvd.nist.gov/vuln/detail/CVE-2022-46823
BDU:2023-00348 **CVE-2022-35256** Уязвимость анализатора HTTP-кода llhttp программного обеспечения для управления сетевой инфраструктурой SINEC INS (Infrastructure Network Services) связана с возможностью обхода механизма аутентификации.	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: ограничение подключения к программному продукту из сетей общего пользования (Интернет);

Идентификатор и описание	Возможные меры защиты
Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код	сегментирование сети с целью ограничения доступа к промышленному сегменту из других подсетей; применение средств межсетевого экранирования уровня веб-приложений. Использование рекомендаций производителя: https://cert-portal.siemens.com/productcert/pdf/ssa-332410.pdf
BDU:2023-00351 **CVE-2023-22964** Уязвимость реализации механизма процедуры аутентификации по протоколу LDAP системы управления IT-службами Zoho ManageEngine ServiceDesk Plus связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: отключение LDAP-аутентификации; использование средств межсетевого экранирования для ограничения возможности удаленного доступа. Источники информации: https://nvd.nist.gov/vuln/detail/CVE-2023-22964 https://www.manageengine.com/products/service-desk-msp/cve-2023-22964.html
BDU:2023-00392 **CVE-2023-0471** Уязвимость компонента WebTransport браузера Google Chrome связана с использованием памяти после её освобождения. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, выполнить произвольный код	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: использование средств антивирусной защиты с функцией контроля доступа к веб-ресурсам; контролируемый доступ в сеть Интернет – регламентация разрешенных сетевых ресурсов и соединений; запуск веб-браузера от имени пользователя с минимальными возможными привилегиями в операционной системе; использование альтернативных веб-браузеров; применение систем обнаружения и предотвращения вторжений. Использование рекомендаций производителя: https://chromereleases.googleblog.com/2023/01/stable-channel-update-for-desktop_24.html
BDU:2023-00393 **CVE-2022-31706** Уязвимость средства управления журналами vRealize Log Insight и платформы виртуализации VMware Cloud Foundation связана с возможностью обхода каталога. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: 1. Загрузить файл KB90635.zip (https://customerconnect.vmware.com/en/downloads/details?downloadGroup=VRLI-8102&productId=1034&rPId=100036). 2. Войти в узел vRealize Log Insight под root пользователем через SSH (используя Putty.exe или любой аналогичный SSH-клиент). 3. Загрузить скрипт KB90635.sh в папку /opt/vmware/bin/ с помощью WinSCP или аналогичной утилиты. 4. Изменить права доступа к файлу и сделать его исполняемым, выполнив приведенные ниже команды: *chmod +x /opt/vmware/bin/KB90635.sh* *chmod 755 /opt/vmware/bin/KB90635.sh*

Идентификатор и описание	Возможные меры защиты
	5. Выполните скрипт, передав аргумент «setup»: */opt/vmware/bin/KB90635.sh setup* 6. Процедуру повторить для всех узлов кластера. Использование рекомендаций производителя: https://www.vmware.com/security/advisories/VMSA-2023-0001.html
BDU:2023-00394 **CVE-2023-0472** Уязвимость реализации технологии WebRTC браузера Google Chrome связана с использованием памяти после её освобождения. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, выполнить произвольный код	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: использование средств антивирусной защиты с функцией контроля доступа к веб-ресурсам; контролируемый доступ в сеть Интернет – регламентация разрешенных сетевых ресурсов и соединений; запуск веб-браузера от имени пользователя с минимальными возможными привилегиями в операционной системе; использование альтернативных веб-браузеров; применение систем обнаружения и предотвращения вторжений. Использование рекомендаций производителя: https://chromereleases.googleblog.com/2023/01/stable-channel update-for-desktop_24.html
BDU:2023-00395 **CVE-2022-31704** Уязвимость средства управления журналами vRealize Log Insight и платформы виртуализации VMware Cloud Foundation связана с ошибками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: 1. Загрузить файл KB90635.zip (https://customerconnect.vmware.com/en/downloads/details?downloadGroup=VRLI-8102&productId=1034&rPId=100036). 2. Войти в узел vRealize Log Insight под root пользователем через SSH (используя Putty.exe или любой аналогичный SSH-клиент). 3. Загрузить скрипт KB90635.sh в папку /opt/vmware/bin/ с помощью WinSCP или аналогичной утилиты. 4. Изменить права доступа к файлу и сделать его исполняемым, выполнив приведенные ниже команды: *chmod +x /opt/vmware/bin/KB90635.sh* *chmod 755 /opt/vmware/bin/KB90635.sh* 5. Выполнить скрипт, передав аргумент «setup»: */opt/vmware/bin/KB90635.sh setup* 6. Процедуру повторить для всех узлов кластера. Использование рекомендаций производителя: https://www.vmware.com/security/advisories/VMSA-2023-0001.html
BDU:2023-00439 **CVE-2023-23560** Уязвимость веб-сервиса New Lexmark Devices принтеров Lexmark связана с недостаточной проверкой запросов на стороне	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.0) CVSS v3:AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Идентификатор и описание	Возможные меры защиты
сервера. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	Компенсирующие меры: отключение веб-сервисов на устройстве путём блокировки доступа к 65002 TCP-порту; использование средств межсетевого экранирования для ограничения удалённого доступа к устройству. Использование рекомендаций производителя: https://publications.lexmark.com/publications/security-alerts/CVE-2023-23560.pdf
BDU:2023-00525 **CVE-2022-27596** Уязвимость операционных систем QTS и QuTS hero связана с возможностью внедрения команд. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Критический (9.8) CVSS v3:AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: ограничение доступа к устройствам Qnap из общедоступных сетей (Интернет); использование средств межсетевого экранирования уровня веб-приложений. Источники информации: https://www.qnap.com/en/security-advisory/qsa-23-01 https://nvd.nist.gov/vuln/detail/CVE-2022-27596
BDU:2023-00526 **CVE-2022-4254** Уязвимость пакета libsss_certmap сервиса управления доступом к удаленным каталогам и механизма аутентификации sssd связана с невозможностью очистки данных сертификата при использовании LDAP-фильтрации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Высокий (8.8) CVSS v3:AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: сброс настроек FreeIPA до конфигурации по умолчанию; отключение неиспользуемых учетных записей, а также учетных записей недоверенных пользователей корневой операционной системы; ограничение доступа к командной строке для недоверенных пользователей; минимизация пользовательских привилегий. Использование рекомендаций производителя: https://access.redhat.com/security/cve/cve-2022-4254
BDU:2023-00528 **CVE-2023-23477** Уязвимость сервера приложений IBM WebSphere Application Server связана с ошибками при обработке сериализованных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Высокий (8.1) CVSS v3:AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: ограничение доступа из общедоступных сетей (Интернет); использование средств межсетевого экранирования для ограничения удаленного доступа к серверу приложений. Источники информации: https://www.ibm.com/support/pages/node/6891111 https://www.cybersecurity-help.cz/vdb/SB2023013137
BDU:2023-00529 **CVE-2023-0430** Уязвимость почтового клиента Thunderbird связана с ошибками	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Идентификатор и описание	Возможные меры защиты
при проверке подписи S/Mime OSCP-сертификата. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, реализовать спуфинг-атаку	Уровень опасности: Высокий (8.8) CVSS v3:AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Компенсирующие меры: использование антивирусного программного обеспечения с функцией антиспуфинг; использование средств межсетевого экранирования для ограничения доступа к недоверенным ресурсам и перехода по нежелательным ссылкам. Использование рекомендаций производителя: https://www.mozilla.org/en-US/security/advisories/mfsa2023-04/
BDU:2023-00549 **CVE-2023-20076** Уязвимость программной платформы Cisco IOx существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнять произвольные команды в операционной системе с привилегиями root-пользователя	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Высокий (7.2) CVSS v3:AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Компенсирующие меры: отключение функции Cisco IOx путём ввода команды:*no iox;* проверка 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 (IOxman):Running* *IOx service (Sec storage):Running* *Libvirtd 5.5.0: Running* ***Dockerd v19.03.13-ce :Running*** *Sync Status: Disabled* Источники информации: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL https://www.helpnetsecurity.com/2023/02/01/cve-2023-20076/
BDU:2023-00550 **CVE-2022-40224** Уязвимость веб-сервера микропрограммного обеспечения Ethernet–коммутатора Moxa SDS-3008 связана с недостаточным объемом ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании путем отправки специально сформированного HTTP-запроса	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Уровень опасности: Высокий (8.6) CVSS v3:AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H Компенсирующие меры: применение систем обнаружения и предотвращения вторжений; сегментирование сетей для ограничения доступа к промышленному оборудованию из других подсетей; использование средств межсетевого экранирования уровня веб-приложений. Использование рекомендаций производителя: https://www.moxa.com/en/support/product-support/security-advisory/sds-3008-series-multiple-web-vulnerabilities