



ФСТЭК РОССИИ

УПРАВЛЕНИЕ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И
ЭКСПОРТНОМУ КОНТРОЛЮ
ПО ДАЛЬНЕВОСТОЧНОМУ
ФЕДЕРАЛЬНОМУ ОКРУГУ

Ул. Ленина, д. 37, г. Хабаровск, 680030

Тел., факс (4212) 35-11-08

E-mail: dfo@fstec.ru

09.06.2025 г. № 9/2313

На № _____

Председателям Советов
по информационной безопасности
при главах высших исполнительных
органов государственной власти
субъектов Российской Федерации
в Дальневосточном федеральном округе

О мерах по повышению защищенности
информационной инфраструктуры

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. Для указанных далее уязвимостей имеется информация о наличии средств их эксплуатации, а также об их использовании в реальных атаках на информационную инфраструктуру.

В соответствии с подпунктом «е» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей, просим обратить внимание на необходимость устранения следующих уязвимостей:

1. Уязвимость функции `soap_message_headers_get_content_disposition()` библиотеки `libsoap` графического интерфейса GNOME (BDU:2025-06242, уровень опасности по CVSS 3.1 – высокий), связанная с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании путем отправки специально сформированного POST-запроса.

В целях предотвращения возможности эксплуатации данной 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 уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty>).

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

использовать схему доступа по «белым» спискам IP-адресов для ограничения возможности эксплуатации уязвимости;

использовать средства межсетевого экранирования для фильтрации сетевого трафика;

использовать виртуальные частные сети для организации удаленного доступа.

2. Уязвимость обработчика JavaScript-сценариев V8 браузера Google Chrome (BDU:2025-06341, уровень опасности по CVSS 3.1 – высокий), связанная с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с помощью специально созданной HTML-страницы.

3. Уязвимость компонента обработки сценариев Scripting Engine браузера Edge и Internet Explorer операционных систем Windows (BDU:2025-05436, уровень опасности по CVSS 3.1 – высокий), связанная с ошибками смещения типов данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально созданной ссылки.

В целях предотвращения возможности эксплуатации указанных в пунктах 2-3 уязвимостей 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 уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty>).

4. Уязвимость функции `getIterator` файла `symfony\finder\Iterator\SortableIterator.php` PHP фреймворка Yii (BDU:2025-06237, уровень опасности по CVSS 3.1 – высокий), связанная с недостатками механизма десериализации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем внедрения специально сформированных данных.

В целях предотвращения возможности эксплуатации данной 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 уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty>).

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

использовать средства межсетевого экранирования уровня веб-приложений для ограничения возможности эксплуатации уязвимости;

ограничить (при возможности) доступ к пользовательским интерфейсам приложения (API-интерфейсам) и иным точкам входа в уязвимое веб-приложение;

использовать средства мониторинга и регистрации событий для обнаружения попыток эксплуатации уязвимости, связанных с десериализацией данных.

5. Уязвимость функций «Print» и «Export Word» программного продукта обработки данных Atlassian Jira Service Management Data Center and Server (BDU:2025-06344, уровень опасности по CVSS 3.1 – высокий), позволяющая нарушителю повысить свои привилегии.

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 уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty>).

В случае невозможности установки обновления программного обеспечения рекомендуется ограничить доступ недоверенных пользователей к программному обеспечению сторонними средствами защиты с использованием технологии «белых» или «черных» списков.

6. Уязвимость функции загрузки образов операционной системы на точки доступа (AP) по внешнему каналу операционной системы Cisco IOS XE (BDU:2025-05297, уровень опасности по CVSS 3.0 – критический), связанная с наличием жестко закодированного JSON Web Token (JWT). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнять произвольные команды путем отправки специально сформированных HTTPS-запросов.

В целях предотвращения возможности эксплуатации данной 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 уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г. (<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty>).

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

- отключить функцию загрузки образов операционной системы на точки доступа (AP) по внешнему каналу;

- использовать средства межсетевого экранирования уровня приложений для фильтрации HTTP-трафика;

- осуществить сегментацию сети с целью ограничения доступа к уязвимому устройству из других подсетей;

- использовать системы обнаружения и предотвращения вторжений для обнаружения (выявления, регистрации) и реагирования на попытки эксплуатации уязвимостей;

- использовать SIEM-системы для отслеживания попыток эксплуатации уязвимостей;

- ограничить доступ к устройству из внешней сети «Интернет».

Прошу организовать контроль реализации указанных рекомендаций в государственных информационных системах указанных органов (организаций).

Прошу до 5 июля 2025 г. проинформировать Управление письмом с электронным вложением в формате PDF по адресу электронной почты dfo_otd9@fstec.ru:

- о результатах выполнения рекомендаций исполнительными органами, органами местного самоуправления и подведомственными им организациями;


- о реализации рекомендаций в государственных информационных системах.

Руководитель Управления



В.Цалко

Исп. и отп. Комарова Т.А.
тел. (4212) 35-11-75
09.06.2025


09.06.2025