ЭЛЕКТРОННОЕ СООБЩЕНИЕ

ФСТЭК РОССИИ

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

Красный проспект, д. 41, г. Новосибирск, 630091
тел./ факс: (383) 203-54-07
E-mail: sfo@fstec.ru
ОКПО 56009786, ОГРН 1025401918761
ИНН/КПП 5405213849/540601001

Руководителям штабов
по обеспечению кибербезопасности
субъектов Российской Федерации

06 декабря 2022 № 2262

О мерах 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 драйвера файловой системы журнала операционных систем Windows (BDU:2022-06934, уровень опасности по CVSS 2.0 – средний уровень опасности, по CVSS 3.0 – высокий уровень опасности), связанной с записью за границами буфера в памяти. Эксплуатация указанной уязвимости может позволить нарушителю выполнить произвольный код с системными привилегиями.

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).

3
020

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

использовать антивирусные средства для детектирования и нейтрализации программ, эксплуатирующих уязвимость;

ограничить доступ к устройствам из корпоративной и интернет-сети с использованием сертифицированных межсетевых экранов, и систем обнаружения вторжений;

использовать многофакторную аутентификацию для удаленного доступа.

Руководитель Управления В.Булгаков