ФСТЭК РОССИИ
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО ДАЛЬНЕВОСТОЧНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
Ленина, д. 37, г. Хабаровск, 680030
Тел., факс (4212) 35-11-08
E-mail: dfo@fstec.ru

06.07.2022 г. № 2/1899

На № _____

Первому вице-губернатору
Хабаровского края,
председателю Совета по
информационной безопасности
при Губернаторе Хабаровского края
А.А.НИКИТИНУ

main@adm.khv.ru

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Уважаемый Александр Александрович!

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 следующей уязвимости:

Уязвимость функции nft_set_desc_concat_parse() ядра Linux (BDU:2022-04090, уровень опасности по CVSS 2.0 — критический уровень опасности, по CVSS 3.0 — критический уровень опасности), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании или выполнить произвольный код.

В целях предотвращения возможности эксплуатации указанной уязвимости необходимо принять следующие меры:

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

ограничить доступ к командной строке для недоверенных пользователей;

использовать антивирусные средства защиты;

осуществлять мониторинг действий пользователей;

использовать системы управления доступом (такие, как SELinux, AppArmor и другие системы управления доступа).

С уважением,

Руководитель Управления В.Цалко