



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

29.06.2022 г. № 2/1809

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 уязвимости программного обеспечения для унификации и упрощения доступа к базам данных Spring Data MongoDB (BDU:2022-03714, уровень опасности по CVSS 2.0 — критический уровень опасности, по CVSS 3.0 — критический уровень опасности), связанной с ошибками при обработке SpEL-выражений. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированного SpEL-запроса.

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

использование символов «[0]» вместо «?0» при написании запроса;
проверка параметров перед вызовами метода запроса;
переконфигурирование BeanPostProcessor с ограничением
QueryMethodEvaluationContextProvider.

Руководитель Управления



В.Цалко