ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000395
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«05» декабря 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за ноябрь 2023 г.»

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня защиты информации при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) служба информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) рекомендует it-специалистам наших клиентов (организаций и индивидуальных предпринимателей) применять в своей работе рекомендации по защите информации, указанные в Приложении 1 к данному письму. В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в службу информационной безопасности по номерам 8(8722) 51-70-44 или направить письмо по электронной почте office@psib.ru .

Председатель Правления _____ **Абдурахманов К.А.**
подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за ноябрь 2023 г.»

На компьютере, с использованием которого осуществляется работа в системе ДБО «iBank2», не рекомендуется устанавливать программное обеспечение, имеющее уязвимости с критичным уровнем опасности. К такому программному обеспечению относится программное обеспечение, указанное в таблице ниже:

№	Наименование уязвимого программного Обеспечения	Идентификатор уязвимостей	Описание уязвимости	Дата выявления	Ссылка на источники	Наличие обновлений
1.	Выполнение произвольного кода в D-Link DAR-7000	CVE-2023-42406	выполнение произвольного кода Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	2023-10-30	http://github.com/flyyue2001/cve/blob/main/D-LINK%20-DAR-7000_sql_:sysmanage:editrole.php.md • http://github.com/1dreamGN/CVE/blob/main/CVE-2023-42406.md	Есть
2.	Выполнение произвольного кода в Microsoft Exchange Server	None	Способ эксплуатации: Отправка специально созданных HTTP-запросов. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	2023-11-02	http://www.zerodayinitiative.com/advisories/ZDI-23-1578/	Есть
3.	Межсайтовый скриптинг в Bitrix24	CVE-2023-1720	Способ эксплуатации: Отправка специально созданного вредоносного файла. Последствия эксплуатации: межсайтовый скриптинг Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-11-01	https://starlabs.sg/advisories/23/23-1720/ • https://bdu.fstec.ru/vul/2023-07458	Есть

	Отказ в обслуживании в Bitrix24	CVE-2023-1718	Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки. Последствия эксплуатации: отказ в обслуживании Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-11-01	https://starlabs.sg/advisories/23/23-1718/ • https://bdu.fstec.ru/vul/2023-07460	Есть
5.	Выполнение произвольного кода в Microsoft Edge	CVE-2023-5996	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-11-10	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-5996	Есть
6.	Выполнение произвольного кода в PostgreSQL	CVE-2023-5869	Способ эксплуатации: Отправка специально сформированных данных. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков	2023-11-09	http://www.postgresql.org/about/news/postgresql-161-155-1410-1313-1217-and-1122-released-2749/	Есть