ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000039 5
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«10» июля 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за июнь 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 июнь 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 Ubuntu	CVE-2023-24540	Способ эксплуатации: Отправка специально созданных запросов. 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.	2023-06-06	http://ubuntu.com/security/notices/USN-6140-1	Есть
2.	Отказ в обслуживании в Ubuntu	CVE-2023-24537	Способ эксплуатации: Не определено. 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.	2023-06-06	http://ubuntu.com/security/notices/USN-6140-1	Есть
3.	Выполнение произвольного кода в D-Link DIR-605L version 1.17B01 BETA	CVE-2023-29961	Способ эксплуатации: Отправка специально сформированных данных. Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.	2023-05-16	https://github.com/Archerber/bug_submit/blob/main/D-Link/dir605l.md	Есть
4.	Выполнение произвольного кода в Tenda AC5 router V15.03.06.28	CVE-2023-31587	Способ эксплуатации: Не определено. Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.	2023-05-16	https://github.com/yanbushuang/CVE/blob/main/TendaAC5.md https://www.tenda.com.cn/download/detail-2740.html https://www.tenda.com.cn/product/AC5.html	Есть
5.	Повышение привилегий в Visual Studio	CVE-2023-29011	Способ эксплуатации: Отправка специально созданного вредоносного файла. 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.	2023-06-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29011	Есть
6.	Выполнение произвольного кода в Windows Server	CVE-2023-29366	Способ эксплуатации: Отправка специально сформированных данных. 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.	2023-06-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-29366	Есть

7.	Выполнение произвольного кода в Microsoft Office	CVE-2023-33146	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. 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.	2023-06-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-33146	Есть