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

«03» мая 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за апрель 2024 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 апрель 2024 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 Google Chrome	CVE-2024-2887	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.	2024-03-27	http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html http://crbug.com/330588502	Есть
2.	Отказ в обслуживании в PHP	CVE-2024-2757	Способ эксплуатации: Отправка специально сформированных данных. 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.	2024-04-11	http://www.php.net/ChangeLog-8.php	Есть
3.	Межсайтовый скриптинг в Microsoft Outlook for Windows	CVE-2024-20670	Способ эксплуатации: Не определено Последствия эксплуатации: Межсайтовый скриптинг Рекомендации по устранению: Данная уязвимость устраняется	2024-04-10	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20670	Есть

			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.			
4.	Выполнение произвольного кода в Microsoft Excel	CVE-2024-26257	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. 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.	2024-04-10	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257	Есть
5.	Обход безопасности в Microsoft Windows	CVE-2024-29988	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. Последствия эксплуатации: Обход безопасности 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.	2024-04-09	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988 http://www.zerodayinitiative.com/blog/2024/4/9/the-april-2024-security-updates-review http://www.zerodayinitiative.com/advisories/ZDI-24-361/ https://bdu.fstec.ru/vul/2024-02831	Есть
6.	Выполнение произвольного кода в D-Link routers	CVE-2024-3273	Способ эксплуатации: Отправка специально сформированных данных. Последствия эксплуатации: Выполнение произвольного кода Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетев.экранирования или другими административными мерами.	2024-04-08	http://vuldb.com/?id.259284 http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383 https://bdu.fstec.ru/vul/2024-02740	Есть