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

«30» сентября 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за август 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 _____ **К.А.Абдурахманов**
подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за август 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.	Межсайтовый скриптинг в Twisted Web	CVE-2024-41671	Способ эксплуатации: Отправка специально созданных HTTP-запросов. 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.	2024-07-30	http://github.com/twisted/twisted/security/advisories/GHSA-c8m8-j448-xjx7 http://github.com/twisted/twisted/commit/046a164f89a0f08d3239ecebd750360f8914df33 http://github.com/twisted/twisted/commit/4a930de12fb67e88fefcb8822104152f42b27abc	Есть
2.	Выполнение произвольного кода в Google Chrome и Microsoft Edge	CVE-2024-6990	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия эксплуатации: Выполнение произвольного кода	2024-08-01	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-6990	Есть

			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.			
3.	Выполнение произвольного кода в Django	CVE-2024-42005	Способ эксплуатации: Отправка специально созданных запросов. 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.	2024-08-07	http://www.djangoproject.com/weblog/2024/aug/06/security-releases/	Есть
4.	Обход безопасности в Mozilla Thunderbird	CVE-2024-7529	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия эксплуатации: Выполнение произвольного кода	2024-08-07	http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/	Есть

			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.			
5.	Повышение привилегий в Docker	CVE-2024-41110 BDU:2024-05760	Способ эксплуатации: Отправка специально сформированного запроса. Последствия эксплуатации: Повышение привилегий 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.	2024-08-03	https://bdu.fstec.ru/vul/2024-05760	Есть
6.	Выполнение произвольного кода в Microsoft PowerPoint	CVE-2024-38171	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. Последствия эксплуатации: Выполнение произвольного кода	2024-08-14	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171 http://www.zerodayinitiative.com/advisories/ZDI-24-1148/	Есть

			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.			
7.	Выполнение произвольного кода в Adobe Photoshop	CVE-2024-34117	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.	2024-08-13	http://helpx.adobe.com/security/products/photoshop/apsb24-49.html	Есть