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

«01» октября 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за сентябрь 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 сентябрь 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 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
2.	Выполнение произвольного кода в Microsoft Edge	CVE-2024-43496	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия эксплуатации: Выполнение	2024-09-20	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43496	Есть

			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.			
3.	Выполнение произвольного кода в Microsoft Office Visio	CVE-2024-38016	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.	2024-09-19	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38016	Есть
4.	Получение конфиденциальной информации в Google Chrome и	CVE-2024-8907	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия	2024-09-18	http://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_17.html http://crbug.com/360642942 http://msrc.microsoft.com/	Есть

	Microsoft Edge		эксплуатации: Получение конфиденциальной информации 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.		update-guide/en-US/advisory/CVE-2024-8907	
5.	Выполнение произвольного кода в D-Link wireless routers	CVE-2024-45698	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.	2024-09-17	http://www.twcert.org.tw/tw/cp-132-8090-bf06b-1.html http://www.twcert.org.tw/en/cp-139-8091-bcd52-2.html http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412	Есть
6.	Выполнение произвольного кода в Adobe Photoshop	CVE-2024-45108	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. Последствия эксплуатации: Выполнение произвольного кода	2024-09-10	http://helpx.adobe.com/security/products/photoshop/apsb24-72.html	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 Acrobat and Reader**	**CVE-2024-41869**	**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.**	**2024-09-10**	**http://helpx.adobe.com/security/products/acrobat/apsb24-70.html**	**Есть**