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» апреля 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за март 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 март 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 Microsoft Edge	CVE-2024-1939	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.	2024-02-29	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1939	Есть
2.	Отказ в обслуживании в Cisco NX-OS Software	CVE-2024-20321	Способ эксплуатации: Отправки специально сформированного eBGP-трафика 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.	2024-02-29	http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ https://bdu.fstec.ru/vul/2024-01671	Есть
3.	Выполнение произвольного кода в D-Link Dir 816	CVE-2023-24331	Способ эксплуатации: Отправка специально сформированных данных. Последствия эксплуатации: выполнение произвольного кода	2024-02-27	http://github.com/caoyebo/CVE/tree/main/Dlink%20816%20-%20CVE-2023-24331	Есть

			Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.			
4.	Получение конфиденциальной информации в Apple macOS Ventura	CVE-2024-23227	Способ эксплуатации: Не определено Последствия 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.	2024-03-07	http://support.apple.com/en-us/HT214085	Есть
5.	Выполнение произвольного кода в Foxit PDF Editor for Mac	None	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.	2024-03-08	http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+for+Mac+2024.1+and+Foxit+PDF+Reader+for+Mac+2024.12024-03-05+00%3A00%3A00	Есть
6.	Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows	CVE-2024-25858	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	2024-03-08	http://www.foxit.com/support/security-bulletins.html	Есть

			Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.			
7.	Выполнение произвольного кода в Google Chrome	CVE-2024-2176	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.	2024-03-06	http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop.html http://crbug.com/325936438	Есть
8.	Выполнение произвольного кода в VMware ESXi, VMware Workstation and Fusion	CVE-2024-22252	Способ эксплуатации: Не определено 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.	2024-03-05	http://www.vmware.com/security/advisories/VMSA-2024-0006.html https://bdu.fstec.ru/vul/2024-01807	Есть