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

«02» марта 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за февраль 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) 67-72-75, 8(8722) 62-16-94 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 февраль 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 Microsoft Exchange Server	CVE-2023-21706	Способ эксплуатации: Отправка специально созданного запроса.	2023-02-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21706	Есть
2.	Выполнение произвольного кода в Microsoft Office	CVE-2023-21716	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. Выполнение операций за пределами буфера памяти	2023-02-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21716	Есть
3.	Повышение привилегий в Visual Studio	CVE-2023-21566	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями	2023-02-15	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21566	Есть
4.	Выполнение произвольного кода в Windows	CVE-2023-21695	Способ эксплуатации: Отправка специально созданного запроса. CWE-20 Некорректная проверка входных данных	2023-02-14	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21695	Есть
5.	Выполнение произвольного кода в Windows	CVE-2023-21689	Способ эксплуатации: Отправка специально созданных запросов. CWE-20 Некорректная проверка входных данных	2023-02-14	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689	Есть
6.	Выполнение произвольного кода в Windows	CVE-2023-21690	Способ эксплуатации: Отправка специально созданных запросов. CWE-20 Некорректная проверка входных данных	2023-02-14	http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21690	Есть
7.	Выполнение произвольного кода в Visual Studio	CVE-2023-23381	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. CWE-119 Выполнение операций за пределами буфера памяти	2023-02-15	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23381	Есть
8.	Получение конфиденциальной информации в Windows	CVE-2023-21691	Способ эксплуатации: Отправка специально созданного запроса.CWE-125 Чтение за пределами буфера	2023-02-14	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21691	Есть
9.	Повышение привилегий в Уязвимый продукт Windows	CVE-2023-21823	Способ эксплуатации: • Открытие пользователем специально созданного вредоносного файла.CWE-119 Выполнение операций за пределами буфера памяти	2023-02-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21823	Есть
10.	Отказ в обслуживании в Windows	CVE-2023-21701	Способ эксплуатации: Отправка специально сформированных данных.CWE-20 Некорректная проверка входных данных	2023-02-14	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21701	Есть