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

«03» октября 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за сентябрь 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) 51-70-44 или направить письмо по электронной почте office@psib.ru .

Председатель Правления _____ **Абдурахманов К.А.**
подпись

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.	Уязвимость в сервисе видеоконференций	ALRT-20230906.1	По каналам НКЦКИ поступают сведения об участившихся компьютерных инцидентах, связанных с эксплуатацией уязвимости в сервисе видеоконференций iMind. Эксплуатация указанной уязвимости позволяет злоумышленнику выполнить произвольный код от имени администратора и получить несанкционированный доступ к данным в целевой системе. Уязвимость на данный момент не имеет идентификатора. Признаком эксплуатации уязвимости может быть запуск команды « » от имени системной сервисной учетной записи «monitoring». Во время перезапуска веб-сервера происходит установка вредоносных модулей от имени процесса « ».	06.09.2023	-	Есть
2.	Выполнение произвольного кода в ASUS Routers	CVE-2023-39240	Выполнение произвольного кода. 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.	2023-09-06	http://www.hkcert.org/security-bulletin/asus-router-multiple-vulnerabilities_20230906 http://www.twcert.org.tw/tw/cp-132-7356-021bf-1	Есть
3.	Выполнение произвольного кода в Linux kernel	CVE-2023-32257	Выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой	2023-09-06	http://bugzilla.redhat.com/show_bug.cgi?id=2219806 http://github.com/torvalds/linux/commit/f5c779b7ddbda30866cf2a27c63e34158f858c73	Ест

			и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.		http://www.zerodayinitiative.com/advisories/ZDI-23-705/ https://bdu.fstec.ru/vul/2023-02742	
4.	Выполнение произвольного кода в Notepad++	CVE-2023-40031	Выполнение произвольного кода. 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.	2023-09-08	http://github.com/notepad-plus-plus/notepad-plus-plus/releases/tag/v8.5.7 http://securitylab.github.com/advisories/GHSL-2023-092_Notepad__/ http://github.com/notepad-plus-plus/notepad-plus-plus/issues/14073 http://notepad-plus-plus.org/news/v857-released-fix-security-issues/ https://bdu.fstec.ru/vul/2023-05051	Есть
5.	Выполнение произвольного кода в Microsoft Edge	CVE-2023-4763	Открытие пользователем специально созданной вредоносной веб-страницы. 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.	2023-09-07	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-4763 https://bdu.fstec.ru/vul/2023-05249	Есть
6.	Отказ в обслуживании в D-Link DIR-880	CVE-2023-39669	Способ эксплуатации: Не определено. Последствия эксплуатации: Отказ в обслуживании. Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	2023-08-25	https://nvd.nist.gov/vuln/detail/CVE-2023-39669 https://bdu.fstec.ru/vul/2023-04863	Есть
7.	Выполнение произвольного кода в Tenda routers	CVE-2023-38940	Способ эксплуатации: Не определено. Последствия эксплуатации: Выполнение произвольного кода. Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	2023-08-09	https://nvd.nist.gov/vuln/detail/CVE-2023-38940	Есть

8.	Выполнение произвольного кода в Chrome OS	CVE-2023-4427	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.	2023-09-19	http://chromereleases.googleblog.com/2023/09/long-term-support-channel-update-for_18.html https://bdu.fstec.ru/vul/2023-04907	Есть