ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000039 5
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«11» января 2023 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за декабрь 2022 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 _____ **К.А.Абдурахманов**
подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за декабрь 2022 г.»

Зафиксирован факт распространения вредоносного программного обеспечения, классифицируемого различными антивирусными решениями как «HEUR:Trojan-Downloader.MSOffice.Dotmer.gen».

Основные индикаторы компрометации

1.	**URL-адреса и IP-адреса, к которым производятся обращения**	**hxxp://msys[.]su/microsoft-office-word/t.php?t=3da82cafc9918a32d03e1103f7e4711d40a4c743f483eba5b370bedd2b8476e3cab73565b3d28350b9ece3d403c9f0b1&action=show_document&z=sudrf&x=5000lformats.org/dratargetmodeexternalocessingdrawingxmlns:w10urn:schemas-microsoft-com:office:wordxmlns:w** **78.24.221[.]94** **209.197.3[.]8**
2.	**Адреса и домены отправителей писем**	**urgansky.krg@sudrf[.]ru**

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.	Эксплуатация уязвимости SPNEGO NEGOEX (CVE-2022-37958)	T1203. Уязвимости в клиентском ПО	Уязвимость SPNEGO NEGOEX (CVE-2022-37958) находится в механизме безопасности расширенного согласования SPNEGO (NEGOEX), который позволяет клиенту и серверу согласовывать выбор используемого механизма безопасности. Эта уязвимость представляет собой возможность удаленного выполнения кода перед аутентификацией, затрагивающую широкий спектр	16.12.2022	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37958 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37958 https://securityintelligence.com/posts/critical-remote-code-execution-vulnerabilityspnego-extended-negotiation-security-mechanism/	Есть

			протоколов. Уязвимость позволяет злоумышленникам удаленно выполнять произвольный код, получая доступ к протоколу NEGOEX через любой протокол приложения Windows, который выполняет аутентификацию, например, блок сообщений сервера (SMB) или протокол удаленного рабочего стола (RDP) по умолчанию. Этот список уязвимых протоколов не полный, уязвимость может существовать в любом протоколе, где используется SPNEGO. В том числе в протоколе передачи сообщений (SMTP) и протоколе передачи гипертекста (HTTP), когда включено согласование аутентификации SPNEGO, например, для использования с Kerberos или Net-, NTLM-аутентификациями.			
	Уязвимость компонента Profiles браузера Google Chrome	CVE-2022-4440	Уязвимость компонента Profiles браузера Google Chrome (CVE-2022-4440, уровень опасности по CVSS 3.1 - высокий), связанная с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код.	23.12.2022	-	Есть
	Выполнение произвольного кода в Google Chrome OS	MITRE: CVE-2022-3038	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	1 декабря 2022 г.	https://bdu.fstec.ru/vul/2022-05448 http://chromereleases.googleblog.com/2022/11/long-termsupport-channel-update-for_30.html	Есть
	Выполнение произвольного кода в Microsoft Edge	MITRE: CVE-2022-4135	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	28 ноября 2022 г.	https://bdu.fstec.ru/vul/2022-06993 http://portal.msrc.microsoft.com/en-US/securityguidance/advisory/CVE-2022-4135	Есть