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

«01» июля 2022г. **г. Махачкала**

«Информирование клиентов,системы дистанционного банковского обслуживания «iBank2» о мерах защиты за июнь 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.

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

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за июнь 2022 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.	Недостатки в безопасности системы VipNet	ALRT-20220517.1	По каналам НКЦКИ получена информация о недостатках в безопасности системы VipNet, применяемых злоумышленниками в целенаправленных компьютерных атаках.	17 мая 2022 г.	-	Есть
2.	Эксплуатация RCE-уязвимостей CMS 1С-Битрикс	BDU:2022-01141/CVE-2022-27228	Версии «1С-Битрикс: Управление сайтом» модуль vote до 21.0.100 (2022-03-04) и модуль fileman до 22.0.0 (2022-03-27) подвержены эксплуатации данных уязвимостей	01 июня 2022 г.	https://bdu.fstec.ru/vul/2022-01141 https://dev.1c-bitrix.ru/docs/versions.php?lang=ru&module=vote https://dev.1c-bitrix.ru/docs/versions.php?lang=ru&module=fileman	Есть
3.	Выполнение произвольного кода в продуктах Autodesk	MITRE: CVE-2022-27871	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена ошибкой границ памяти.	01 июня 2022 г.	http://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	Есть
4.	Выполнение произвольного кода в Microsoft Office	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного DOC-файла. Уязвимость обусловлена возможностью запуска настраиваемого поиска.	02 июня 2022 г.	-	Есть
5.	Отказ в обслуживании в Asus DSL-N14U-B1 1.1.2.3_805	MITRE: CVE-2021-3254	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных пакетов. Уязвимость обусловлена некорректным использованием внутренних ресурсов.	11 мая 2022 г.	https://nvd.nist.gov/vuln/detail/CVE-2021-3254	Есть
6.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-2007	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 в компоненте WebGPU.	09 июня 2022 г.	http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1326210 http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1317673 http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1330379	Есть
7.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-2008	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально	09 июня 2022 г.	http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1326210 http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1317673	Есть

			созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти в компоненте WebGL.		http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1330379	
8.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-2011	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 в компоненте ANGLE.	09 июня 2022 г.	http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1326210 http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1317673 http://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html http://crbug.com/1330379	Есть
9.	Выполнение произвольного кода в QNAP QTS update for PHP	MITRE: CVE-2019-11043	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой границ памяти.	23 июня 2022 г.	http://www.qnap.com/en/security-advisory/qsa-22-20	Есть
10.	Множественные уязвимости в Google ChromeOS	MITRE: CVE-2022-1853	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.	28 июня 2022 г.	http://chromereleases.googleblog.com/2022/06/long-term-support-channel-update-for.html	Есть
11.	Множественные уязвимости в Google ChromeOS	MITRE: CVE-2022-1855 CVE-2022-1861	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.	28 июня 2022 г.	http://chromereleases.googleblog.com/2022/06/long-term-support-channel-update-for.html	Есть
12.	Множественные уязвимости в Google ChromeOS	MITRE: CVE-2022-1862	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией аутентификации в расширениях.	28 июня 2022 г.	http://chromereleases.googleblog.com/2022/06/long-term-support-channel-update-for.html	Есть
13.	Выполнение произвольного кода в Foxit PDF Reader and Editor	MITRE: Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена ошибкой использования после освобождения.	28 июня 2022 г.	http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.0+and+Foxit+PDF+Editor+12.01970-01-01+01%3A00%3A00	Есть
14.	Выполнение произвольных команд ОС в Microsoft Office	MITRE: CVE-2022-30190	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды ОС в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой ввода.	30 мая 2022 г.	https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/	Есть