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

«03» июня 2022г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за май 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 май 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. Первый недостаток в безопасности связан с возможностью обхода фильтров в компоненте ПО VipNet Client – «Контроль приложений». Данный компонент позволяет следить за сетевой активностью приложений, а также корректировать ее посредством создания блокирующих правил. Для обхода действующих блокирующих правил злоумышленники отправляют соответствующий код управления драйверу Itcsrf.sys (Itcsrfv64.Sys) в составе ПО VipNet Client. В результате для процесса, PID которого был отправлен на драйвер вместе с управляющим кодом, будет разрешена сетевая активность в обход к примененным правилам компонета «Контроль приложений». Второй недостаток в безопасности связан с возможностью запуска произвольного кода на системе с установленным ПО VipNet Client, путем формирования специального пакета обновлений в центре управления VipNet Administrator и отправки его на подключенные к защищенной сети хосты. Проблема безопасности заключается в том, что в составе комплекса VipNet Client и Vipnet Administrator имеется исполняемый файл LHA.exe, который имеет цифровую подпись INFOTECS и при этом подвержен уязвимости типа DLL (DLL hijacking).	17 мая 2022 г.	-	-
2.	Множественные уязвимости в ПО для процессоров Intel	MITRE: CVE-2021-33123	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректным контролем доступа в модуле кода,	16 мая 2022 г.	-	-

3.	Множественные уязвимости в ПО для процессоров Intel	MITRE: CVE-2021-0190	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена исключением во встроенном ПО BIOS.	16 мая 2022 г.	-	-
4.	Множественные уязвимости в ПО для процессоров Intel	MITRE: CVE-2021-33122	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена недостаточным управлением потоком управления во встроенном ПО BIOS.	16 мая 2022 г.	-	-
5.	Множественные уязвимости в ПО для процессоров Intel	MITRE: CVE-2021-0189	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена использованием для указателя смещения за пределами назначенного диапазона.	16 мая 2022 г.	-	-
6.	Множественные уязвимости в ПО для процессоров Intel	MITRE: CVE-2021-33124	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.	16 мая 2022 г.	-	-
7.	Множественные уязвимости в Mozilla Firefox и Thunderbird	MITRE: CVE-2022-1802	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена загрязнением прототипа.	24 мая 2022 г.	http://www.mozilla.org/en-US/security/advisories/mfsa2022-19/	Есть
8.	Множественные уязвимости в Mozilla Firefox и Thunderbird	MITRE: CVE-2022-1529	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных.	24 мая 2022 г.	http://www.mozilla.org/en-US/security/advisories/mfsa2022-19/	Есть
9.	Множественные уязвимости в продуктах VMWare	MITRE: CVE-2022-22972	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной обработкой запросов проверки пользователей.	24 мая 2022 г.	http://www.vmware.com/security/advisories/VMSA-2022-0014.html http://kb.vmware.com/s/article/88438 http://core.vmware.com/vmsa-2022-0014-questions-answers-faq	Есть
10.	Множественные уязвимости в продуктах VMWare	MITRE: CVE-2022-22973	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольной код с привилегиями root в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности.	24 мая 2022 г.	http://www.vmware.com/security/advisories/VMSA-2022-0014.html http://kb.vmware.com/s/article/88438 http://core.vmware.com/vmsa-2022-0014-questions-answers-faq	Есть
11.	Множественные уязвимости в Google ChromeOS	MITRE: CVE-2021-43527	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.	13 мая 2022 г.	http://chromereleases.googleblog.com/2022/05/long-term-support-channel-update.html	Есть

12.	Множественные уязвимости в Google ChromeOS	MITRE: CVE-2022-23308	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой использования после освобождения.	13 мая 2022 г.	http://chromereleases.googleblog.com/2022/05/long-term-support-channel-update.html	Есть
13.	Множественные уязвимости в Google ChromeOS	MITRE: CVE-2022-1312	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.	13 мая 2022 г.	http://chromereleases.googleblog.com/2022/05/long-term-support-channel-update.html	Есть
14.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-1633 CVE-2022-1634 CVE-2022-1635 CVE-2022-1636 CVE-2022-1639 CVE-2022-1640 CVE-2022-1641	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.	11 мая 2022 г.	http://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html	Есть
15.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-1638	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	13 мая 2022 г.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1634 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1635 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1636 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1637 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1638 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1639 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1640	Есть
16.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-1634 CVE-2022-1635 CVE-2022-1636 CVE-2022-1639 CVE-2022-1640	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.	13 мая 2022 г.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1634 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1635 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1636 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1637 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1638 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1639 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1640	Есть
17.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-1637	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных.	13 мая 2022 г.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1634 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1635 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1636 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1637 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1638 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1639 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-1640	Есть
18.	Множественные уязвимости в Adobe InDesign	MITRE: CVE-2022-28831 CVE-2022-28833	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально	11 мая 2022 г.	http://helpx.adobe.com/security/products/indesign/apsb22-23.html	Есть

			созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.			
19.	Множественные уязвимости в Adobe InDesign	MITRE: CVE-2022-28832	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена пограничной ошибкой при обработке внедренных шрифтов.	11 мая 2022 г.	http://helpx.adobe.com/security/products/indesign/apsb22-23.html	Есть
20.	Выполнение произвольного кода в Foxit PDF Reader and Editor	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена ошибкой смешения типов.	16 мая 2022 г.	http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+11.2.2+and+Foxit+PDF+Editor+11.2.22022-05-09+00%3A00%3A00	Есть
21.	Множественные уязвимости в Zoom	MITRE: CVE-2022-22784	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику отправлять поддельные сообщения с сервера или от имени других пользователей посредством отправки специально сформированного сообщения. Уязвимость обусловлена некорректной проверкой ввода.	24 мая 2022 г.	http://explore.zoom.us/en/trust/security/security-bulletin/#ZSB-22009	Есть
22.	Множественные уязвимости в Zoom	MITRE: CVE-2022-22786	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством установки пользователем специально созданной вредоносной версии обновления. Уязвимость обусловлена некорректной проверкой установленной версии программного обеспечения.	24 мая 2022 г.	http://explore.zoom.us/en/trust/security/security-bulletin/#ZSB-22009	Есть
23.	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