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

«06» декабря 2022г. **г. Махачкала**

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

Вр.и.о. Председателя Правления _____ **Исланов Р.О.**
подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за ноябрь 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.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-3885 CVE-2022-3886 CVE-2022-3887 CVE-2022-3888	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 ноября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3889 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3890 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3888 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3885 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3886 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3887	Есть
2.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-3889	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.	11 ноября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3889 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3890 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3888 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3885 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3886 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3887	Есть
3.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-3890	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	11 ноября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3889 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3890 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3888 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3885 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3886 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3887	Есть
4.	НСД в Dell Technologies PowerProtect Data Domain models: DD3300, DD6400, DD6900/DD9400/ DD9900	MITRE: CVE-2022-24422	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена ошибкой при обработке запросов на аутентификацию.	14 ноября 2022 г.	http://www.dell.com/support/kbdoc/en-us/000199904/dsa-2022-140-dell-technologies-powerprotect-data-domain-security-update-for-idrac9-vnc-console-authentication-vulnerability	Есть
5.	Выполнение произвольного кода в QEMU	MITRE: CVE-2021-3750	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в контексте процесса QEMU на хосте. Уязвимость обусловлена ошибкой использования после освобождения.	15 ноября 2022 г.	http://security.gentoo.org/glsa/202208-27	Есть

6.	Множественные уязвимости в Oracle Database Server	MITRE: CVE-2022-21510	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	1 ноября 2022 г.	http://www.oracle.com/security-alerts/cpujul2022.html?1408	Есть
7.	Множественные уязвимости в Oracle Database Server	MITRE: CVE-2020-35169	Эксплуатация уязвимости позволяет удаленному злоумышленнику манипулировать данными в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	1 ноября 2022 г.	http://www.oracle.com/security-alerts/cpujul2022.html?1408	Есть
8.	Множественные уязвимости в PHP	MITRE: CVE-2022-31630	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику прочитать произвольные файлы в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена граничным условием в функции imageloadfont().	1 ноября 2022 г.	http://bugs.php.net/bug.php?id=81738 http://bugs.php.net/bug.php?id=81739	Есть
9.	Множественные уязвимости в PHP	MITRE: CVE-2022-37454	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением.	1 ноября 2022 г.	http://bugs.php.net/bug.php?id=81738 http://bugs.php.net/bug.php?id=81739	Есть
10.	Множественные уязвимости в VMware Spring Security	MITRE: CVE-2022-31690	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику повысить свои привилегии в целевой системе посредством подделки запроса клиента на сервер авторизации. Уязвимость обусловлена некорректными ограничениями безопасности.	1 ноября 2022 г.	http://tanzu.vmware.com/security/cve-2022-31690 http://tanzu.vmware.com/security/cve-2022-31692	Есть
11.	Множественные уязвимости в VMware Spring Security	MITRE: CVE-2022-31692	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику получить ПСД к целевой системе. Уязвимость обусловлена некорректными правилами авторизации.	1 ноября 2022 г.	http://tanzu.vmware.com/security/cve-2022-31690 http://tanzu.vmware.com/security/cve-2022-31692	Есть
12.	Множественные уязвимости в OpenSSL	MITRE: CVE-2022-3602	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.	1 ноября 2022 г.	http://www.openssl.org/news/secadv/20221101.txt	Есть
13.	Множественные уязвимости в OpenSSL	MITRE: CVE-2022-3786	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных вредоносных данных. Уязвимость обусловлена ошибкой границ памяти.	1 ноября 2022 г.	http://www.openssl.org/news/secadv/20221101.txt	Есть
14.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-3885 CVE-2022-3886 CVE-2022-3887 CVE-2022-3888	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.	9 ноября 2022 г.	http://crbug.com/1375059 http://crbug.com/1372999 http://crbug.com/1380063 http://crbug.com/1380083 http://crbug.com/1372695 http://crbug.com/1377816	Есть
15.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-3889	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия	9 ноября 2022 г.	http://crbug.com/1375059 http://crbug.com/1372999 http://crbug.com/1380063 http://crbug.com/1380083 http://crbug.com/1372695	Есть

			пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.		http://crbug.com/1377816	
16.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-3890	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	9 ноября 2022 г.	http://crbug.com/1375059 http://crbug.com/1372999 http://crbug.com/1380063 http://crbug.com/1380083 http://crbug.com/1372695 http://crbug.com/1377816	Есть
17.	Выполнение произвольного кода в Microsoft Word	MITRE: CVE-2022-41061	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством передачи в приложение специально созданных входных данных. Уязвимость обусловлена некорректной проверкой входных данных.	8 ноября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41061	Есть
18.	Выполнение произвольного кода в Microsoft Office	MITRE: CVE-2022-41107	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	9 ноября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41107	Есть
19.	Выполнение произвольного кода в Visual Studio	MITRE: CVE-2022-41119	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	8 ноября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41119	Есть
20.	Выполнение произвольного кода в Python	MITRE: CVE-2022-42919	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.	16 ноября 2022 г.	http://github.com/python/cpython/issues/97514	Есть