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» ноября 2022г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за октябрь 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  **Абдурахманов К.А.**

подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за октябрь 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-2022-3445 CVE-2022-3449 CVE-2022-3450	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	17 октября 2022 г.	http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1364604 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3445 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1366582 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3447 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1364662 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3449 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1369882	Есть
2.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-3446	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	17 октября 2022 г.	http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1364604 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3445 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1366582 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3447 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1364662 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3449 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1369882	Есть
3.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-3447	Эксплуатация уязвимости позволяет локальному злоумышленнику посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией проверок безопасности.	17 октября 2022 г.	http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1364604 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3445 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1366582 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3447 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1364662 http://portal.msrc.microsoft.com/en-	Есть

					US/security-guidance/advisory/CVE-2022-3449 http://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_11.html http://crbug.com/1369882	
4.	Выполнение произвольных SQL-запросов в WordPress	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	14 сентября 2022 г.	http://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/	Есть
5.	Множественные уязвимости в WhatsApp	MITRE: CVE-2022-36934	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением.	26 сентября 2022 г.	http://www.whatsapp.com/security/advisories/2022/	Есть
6.	Множественные уязвимости в WhatsApp	MITRE: CVE-2022-27492	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного видеофайла. Уязвимость обусловлена некорректной обработкой видеофайла.	26 сентября 2022 г.	http://www.whatsapp.com/security/advisories/2022/	Есть
7.	Выполнение произвольного кода в HP LaserJet Pro printers и PageWide Pro printers and inkjet printers	MITRE: CVE-2022-28721	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.	26 сентября 2022 г.	http://support.hp.com/us-en/document/ish_6839789-6839813-16/HPSBPI03810	Есть
8.	Выполнение произвольного кода в Microsoft Remote Procedure Call Runtime	MITRE: CVE-2022-35830	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.	14 сентября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35830	Есть
9.	Множественные уязвимости в Adobe Photoshop	MITRE: CVE-2022-35713	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	14 сентября 2022 г.	http://helpx.adobe.com/security/products/photoshop/apsb22-52.html	Есть
10.	Множественные уязвимости в Adobe Photoshop	MITRE: CVE-2022-38426 CVE-2022-38427	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена граничной ошибкой при обработке файла.	14 сентября 2022 г.	http://helpx.adobe.com/security/products/photoshop/apsb22-52.html	Есть
11.	Множественные уязвимости в Adobe Photoshop	MITRE: CVE-2022-38429 CVE-2022-38430 CVE-2022-38431	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена граничной ошибкой при обработке файла.	14 сентября 2022 г.	http://helpx.adobe.com/security/products/photoshop/apsb22-52.html	Есть

12.	Множественные уязвимости в Adobe Photoshop	MITRE: CVE-2022-38432 CVE-2022-38433	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена граничной ошибкой при обработке файла.	14 сентября 2022 г.	http://helpx.adobe.com/security/products/photoshop/apsb22-52.html	Есть
13.	Множественные уязвимости в Adobe Photoshop	MITRE: CVE-2022-38434	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения.	14 сентября 2022 г.	http://helpx.adobe.com/security/products/photoshop/apsb22-52.html	Есть
14.	Выполнение произвольного кода в Linux kernel	MITRE: CVE-2022-41674	Эксплуатация уязвимости позволяет аутентифицированному злоумышленнику из смежной сети выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена ошибкой границ памяти.	14 октября 2022 г.	http://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/log/net/mac80211/scan.chttp://www.openwall.com/lists/oss-security/2022/10/13/5http://git.kernel.org/pub/scm/linux/kernel/git/wireless/wireless.git/commit/?id=aebe9f4639b13a1f4e9a6b42cdd2e38c617b442dhttp://bugzilla.suse.com/show_bug.cgi?id=1203770http://www.openwall.com/lists/oss-security/2022/10/13/2	Есть
15.	Выполнение произвольного кода в Microsoft Exchange Server	MITRE: CVE-2022-41082	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	17 октября 2022 г.	http://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html http://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/ http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082 http://www.zerodayinitiative.com/advisories/ZDI-22-1442/	Есть
16.	Выполнение произвольного кода в Windows Server	MITRE: CVE-2022-38044	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы или вредоносного файла. Уязвимость обусловлена целочисленным переполнением.	12 октября 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38044 http://www.zerodayinitiative.com/advisories/ZDI-22-1408/	Есть