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

**«04» октября 2022г.** **г. Махачкала**

**«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за сентябрь 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 сентябрь 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-2022-3053 | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией проверок безопасности. | 1 сентября 2022 г. | http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3038 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3045 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3040 http://crbug.com/1339648 http://crbug.com/1346245 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38012 | Есть |
| 2. | Множественные уязвимости в Microsoft Edge | MITRE: CVE-2022-3039 CVE-2022-3040 CVE-2022-3041 CVE-2022-3046 | 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 сентября 2022 г. | http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3038 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3045 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3040 http://crbug.com/1339648 http://crbug.com/1346245 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38012 | Есть |
| 3. | Множественные уязвимости в Microsoft Edge | MITRE: CVE-2022-38012 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. | 1 сентября 2022 г. | http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3038 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3045 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3040 http://crbug.com/1339648 http://crbug.com/1346245 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38012 | Есть |
| 4. | Множественные уязвимости в Microsoft Edge | MITRE: CVE-2022-3045 | 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. | 1 сентября 2022 г. | http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3038 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3045 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-3040 http://crbug.com/1339648 http://crbug.com/1346245 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-38012 | Есть |
| 5. | Выполнение произвольного кода в Google Chrome | MITRE: CVE-2022-3075 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб- | 3 сентября 2022 г. | http://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html http://crbug.com/1358134 | Есть |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | страницы. Уязвимость обусловлена некорректной проверкой входных данных. | | | |
| 6. | 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 |
| 7. | Выполнение произвольного кода в ImageMagick | MITRE: CVE-2021-20224 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. | 8 сентября 2022 г. | http://github.com/ImageMagick/ImageMagick/commit/5af1dffa4b6ab984b5f13d1e91c95760d75f12a6 http://github.com/ImageMagick/ImageMagick/pull/3083 http://github.com/ImageMagick/ImageMagick6/commit/553054c1cb1e4e05ec86237afef76a32cd7c464d | Есть |
| 8. | Множественные уязвимости в Apple Safari | MITRE: CVE-2022-32886 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. | 12 сентября 2022 г. | http://support.apple.com/en-us/HT213442 | Есть |
| 9. | Множественные уязвимости в Apple Safari | MITRE: CVE-2022-32912 | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена граничной ошибкой при обработке ввода. | 12 сентября 2022 г. | http://support.apple.com/en-us/HT213442 | Есть |
| 10. | Выполнение произвольного кода в Mozilla Firefox и Thunderbird | MITRE: CVE-2022-38477 CVE-2022-38478 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. | 23 августа 2022 г. | http://www.mozilla.org/en-US/security/advisories/mfsa2022-33/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-34/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-36/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-37/ | Есть |
| 11. | 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 |
| 12. | 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 |
| 13. | 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 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14. | 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 |
| 15. | 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 |