ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000395
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«01» декабря 2021г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за ноябрь 2021 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

Исп. Ирганов Ю.Г.
руководитель СИБ
8 (8722) 67-72-75

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за ноябрь 2021 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 Google Chrome	MITRE: CVE-2021-37998 CVE-2021-38002 CVE-2021-37997	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 октября 2021 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37997 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38002 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37999 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38001 http://crbug.com/1259587 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37998 http://crbug.com/1251541 http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html http://crbug.com/1260940 http://crbug.com/1259864 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38000 http://crbug.com/1263462 https://www.cybersecurity-help.cz/vdb/SB2021102808 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38003 http://crbug.com/1260577	Есть
2	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-37999	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 на странице новой вкладки.	28 октября 2021 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37997 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38002 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37999 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38001 http://crbug.com/1259587 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37998 http://crbug.com/1251541 http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html http://crbug.com/1260940 http://crbug.com/1259864 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38000 http://crbug.com/1263462 https://www.cybersecurity-help.cz/vdb/SB2021102808 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38003 http://crbug.com/1260577	Есть
3		MITRE: CVE-2021-38000	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-	28 октября 2021 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37997 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38002 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37999 http://portal.msrc.microsoft.com/en-	Есть

			страницы. Уязвимость обусловлена некорректной реализацией безопасности в движке V8 в Google Chrome.		US/security-guidance/advisory/CVE-2021-38001 http://crbug.com/1259587 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37998 http://crbug.com/1251541 http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html http://crbug.com/1260940 http://crbug.com/1259864 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38000 http://crbug.com/1263462 https://www.cybersecurity-help.cz/vdb/SB2021102808 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38003 http://crbug.com/1260577	
4		MITRE: CVE-2021-38001	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.	28 октября 2021 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37997 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38002 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37999 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38001 http://crbug.com/1259587 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37998 http://crbug.com/1251541 http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html http://crbug.com/1260940 http://crbug.com/1259864 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38000 http://crbug.com/1263462 https://www.cybersecurity-help.cz/vdb/SB2021102808 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38003 http://crbug.com/1260577	Есть
5		MITRE: CVE-2021-38003	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией реализацией безопасности в движке V8 в Google Chrome.	28 октября 2021 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37997 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38002 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37999 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38001 http://crbug.com/1259587 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37998 http://crbug.com/1251541 http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html http://crbug.com/1260940 http://crbug.com/1259864 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38000 http://crbug.com/1263462 https://www.cybersecurity-help.cz/vdb/SB2021102808 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38003 http://crbug.com/1260577	Есть
6	Выполнение произвольного кода в Adobe Character Animator 2021	MITRE: CVE-2021-40763 CVE-2021-40764 CVE-2021-40765 CVE-2021-40767	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных.	1 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021110105 http://helpx.adobe.com/security/products/character_animator/apsb21-95.html	Есть
7	Выполнение произвольного кода в Adobe Premiere Pro	MITRE: CVE-2021-40792 CVE-2021-	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой	27 октября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021102704 http://helpx.adobe.com/security/products/premiere_pro/apsb21-100.html	Есть

		40793 CVE-2021-40794	системе. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных.			
8	Множественные уязвимости в Adobe Bridge CC	MITRE: CVE-2021-42533	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного файла. Уязвимость обусловлена ошибкой границ памяти.	1 ноября 2021 г.	http://helpx.adobe.com/security/products/bridge/apsb21-94.html https://www.cybersecurity-help.cz/vdb/SB2021110106	Есть
9	Множественные уязвимости в Adobe Bridge CC	MITRE: CVE-2021-42729 CVE-2021-42730 CVE-2021-42724	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных.	1 ноября 2021 г.	http://helpx.adobe.com/security/products/bridge/apsb21-94.html https://www.cybersecurity-help.cz/vdb/SB2021110106	Есть
10		MITRE: CVE-2021-42728	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.	1 ноября 2021 г.	http://helpx.adobe.com/security/products/bridge/apsb21-94.html https://www.cybersecurity-help.cz/vdb/SB2021110106	Есть
11	Множественные уязвимости Mozilla Firefox	MITRE: CVE-2021-38504	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения.	2 ноября 2021 г.	http://www.mozilla.org/en-US/security/advisories/mfsa2021-49/ https://www.cybersecurity-help.cz/vdb/SB2021110228 http://www.mozilla.org/en-US/security/advisories/mfsa2021-48/	Есть
12	Множественные уязвимости в D-Link DAP-2020	MITRE: CVE-2021-34861 CVE-2021-34862 CVE-2021-34863 CVE-2021-27248	Эксплуатация уязвимости позволяет злоумышленнику в локальной сети выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.	1 октября 2021 г.	http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201 http://www.zerodayinitiative.com/advisories/ZDI-21-979/ https://www.cybersecurity-help.cz/vdb/SB2021100105 http://www.zerodayinitiative.com/advisories/ZDI-21-978/ http://www.zerodayinitiative.com/advisories/ZDI-21-203/ http://www.zerodayinitiative.com/advisories/ZDI-21-977/ http://www.zerodayinitiative.com/advisories/ZDI-21-204/	Есть
13	Множественные уязвимости в D-Link DAP-2020	MITRE: CVE-2021-27249	Эксплуатация уязвимости позволяет злоумышленнику в локальной сети выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сценариев CGI.	1 октября 2021 г.	http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201 http://www.zerodayinitiative.com/advisories/ZDI-21-979/ https://www.cybersecurity-help.cz/vdb/SB2021100105 http://www.zerodayinitiative.com/advisories/ZDI-21-978/ http://www.zerodayinitiative.com/advisories/ZDI-21-203/ http://www.zerodayinitiative.com/advisories/ZDI-21-977/ http://www.zerodayinitiative.com/advisories/ZDI-21-204/	Есть
14	Множественные уязвимости в Zyxel ZyWALL VPN2S	MITRE: CVE-2021-35027	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольные файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.	4 октября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021100401 http://www.zyxel.com/support/Zyxel_security_advisory_for_directory_traversal_and_command_injection_vulnerabilities_of_VPN2S_Firewall.shtml	Есть

15	Множественные уязвимости в Zyxel ZyWALL VPN2S	MITRE: CVE-2021-35028	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.	4 октября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021100401 http://www.zyxel.com/support/Zyxel_security_advisory_for_directory_traversal_and_command_injection_vulnerabilities_of_VPN2S_Firewall.shtml	Есть
16	Выполнение произвольного кода в QNAP NAS Multimedia Console	MITRE: CVE-2021-38684	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректным определением границ буфера памяти в QNAP NAS с активным компонентом Multimedia Console	12 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021111213 http://www.qnap.com/en/security-advisory/qsa-21-45	Есть
17	Выполнение произвольного кода в Apache Traffic Control	MITRE: CVE-2021-43350	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного POST запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке имен пользователей в Apache Traffic Control Traffic Ops.	12 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021111211 http://trafficcontrol.apache.org/security/ http://www.openwall.com/lists/oss-security/2021/11/11/4 http://www.openwall.com/lists/oss-security/2021/11/11/3	Есть
18	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-38007	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов в компоненте V8.	15 ноября 2021 г.	http://crbug.com/1268274 https://www.cybersecurity-help.cz/vdb/SB2021111601 http://crbug.com/1254189 http://crbug.com/957553 http://crbug.com/1248567 http://crbug.com/1260649 http://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html http://crbug.com/1242392 http://crbug.com/1241091 http://crbug.com/1233375 http://crbug.com/1264477 http://crbug.com/1197889 http://crbug.com/1263620 http://crbug.com/1240593	Есть
19	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-38015 CVE-2021-38021 CVE-2021-38018	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в уязвимом продукте посредством открытия пользователем • специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией проверок безопасности.	15 ноября 2021 г.	http://crbug.com/1268274 https://www.cybersecurity-help.cz/vdb/SB2021111601 http://crbug.com/1254189 http://crbug.com/957553 http://crbug.com/1248567 http://crbug.com/1260649 http://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html http://crbug.com/1242392 http://crbug.com/1241091 http://crbug.com/1233375 http://crbug.com/1264477 http://crbug.com/1197889 http://crbug.com/1263620 http://crbug.com/1240593	Есть
20	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-38014	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных в Swiftshader	15 ноября 2021 г.	http://crbug.com/1268274 https://www.cybersecurity-help.cz/vdb/SB2021111601 http://crbug.com/1254189 http://crbug.com/957553 http://crbug.com/1248567 http://crbug.com/1260649 http://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html http://crbug.com/1242392 http://crbug.com/1241091 http://crbug.com/1233375 http://crbug.com/1264477	Есть

					http://crbug.com/1197889 http://crbug.com/1263620 http://crbug.com/1240593	
21	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-38008 CVE-2021-38011 CVE-2021-38005 CVE-2021-38006	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.	15 ноября 2021 г.	http://crbug.com/1268274 https://www.cybersecurity-help.cz/vdb/SB2021111601 http://crbug.com/1254189 http://crbug.com/957553 http://crbug.com/1248567 http://crbug.com/1260649 http://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html http://crbug.com/1242392 http://crbug.com/1241091 http://crbug.com/1233375 http://crbug.com/1264477 http://crbug.com/1197889 http://crbug.com/1263620 http://crbug.com/1240593	Есть
22	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-38013	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при распознавании отпечатков пальцев.	15 ноября 2021 г.	http://crbug.com/1268274 https://www.cybersecurity-help.cz/vdb/SB2021111601 http://crbug.com/1254189 http://crbug.com/957553 http://crbug.com/1248567 http://crbug.com/1260649 http://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html http://crbug.com/1242392 http://crbug.com/1241091 http://crbug.com/1233375 http://crbug.com/1264477 http://crbug.com/1197889 http://crbug.com/1263620 http://crbug.com/1240593	Есть
23	Повышение привилегий в Microsoft Windows Installer	MITRE: CVE-2021-41379	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности.	9 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021110933 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379	Есть
24	Множественные уязвимости в Wireshark	MITRE: CVE-2021-39924	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданных вредоносных пакетов. Уязвимость обусловлена ошибкой цикла в диссекторе Bluetooth DHT	17 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021111737 http://www.wireshark.org/security/wnpa-sec-2021-07.html http://www.wireshark.org/security/wnpa-sec-2021-09.html http://www.wireshark.org/security/wnpa-sec-2021-08.html http://www.wireshark.org/security/wnpa-sec-2021-11.html http://www.wireshark.org/security/wnpa-sec-2021-14.html http://www.wireshark.org/security/wnpa-sec-2021-13.html http://www.wireshark.org/security/wnpa-sec-2021-10.html http://www.wireshark.org/security/wnpa-sec-2021-12.html http://www.wireshark.org/security/wnpa-sec-2021-15.html	Есть
25	Множественные уязвимости в Wireshark	MITRE: CVE-2021-39920 CVE-2021-39921 CVE-2021-39922 CVE-2021-39925 CVE-2021-39926 CVE-2021-39928 CVE-2021-	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданных вредоносных пакетов. Уязвимость обусловлена некорректной проверкой входных данных.	17 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021111737 http://www.wireshark.org/security/wnpa-sec-2021-07.html http://www.wireshark.org/security/wnpa-sec-2021-09.html http://www.wireshark.org/security/wnpa-sec-2021-08.html http://www.wireshark.org/security/wnpa-sec-2021-11.html http://www.wireshark.org/security/wnpa-sec-2021-14.html http://www.wireshark.org/security/wnpa-sec-2021-13.html	Есть

		39929			http://www.wireshark.org/security/wnpa-sec-2021-10.html http://www.wireshark.org/security/wnpa-sec-2021-12.html http://www.wireshark.org/security/wnpa-sec-2021-15.html	
26	НСД к данным в Microsoft Azure Active Directory	MITRE: CVE-2021-42306	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить НСД к данным в целевой системе. Уязвимость обусловлена некорректным выводом данных	24 ноября 2021 г.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42306 https://www.cybersecurity-help.cz/vdb/SB2021112403	Есть
27	Выполнение произвольного кода в ОС Windows	CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код с привилегиями SYSTEM в целевой системе посредством запуска специально созданного вредоносного файла. Уязвимость обусловлена некорректными разрешениями в установщике Windows.	25 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021112505 http://github.com/klinix5/InstallerFileTakeOver http://blog.talosintelligence.com/2021/11/attackers-exploiting-zero-day.html	Есть
28	Выполнение произвольного кода в TP-Link TL-XVR1800L	CWE-94: Некорректное управление генерированием кода (внедрение кода)	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	29 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021112905 http://thecyberthrone.in/2021/11/26/zeroday-vulnerability-in-tp-link-router/	Есть
29	Множественные уязвимости в Foxit PDF Reader и PhantomPDF	MITRE: CVE-2021-34948 CVE-2021-34949 CVE-2021-34950 CVE-2021-34951 CVE-2021-34952 CVE-2021-34953 CVE-2021-34954 CVE-2021-34955 CVE-2021-34956 CVE-2021-34957 CVE-2021-34958 CVE-2021-34959 CVE-2021-34960 CVE-2021-34961 CVE-2021-34962 CVE-2021-34963 CVE-2021-34964 CVE-2021-34965 CVE-2021-34966 CVE-2021-34967 CVE-2021-34968	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена ошибкой границ памяти.	29 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021112906 http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PhantomPDF+10.1.62021-11-29+00%3A00%3A00	Есть

		CVE-2021-34969 CVE-2021-34971 CVE-2021-34972 CVE-2021-34974 CVE-2021-34975				
30	Выполнение произвольного кода в Kaspersky Password Manager	MITRE: CVE-2021-35052	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии и выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректным управлением привилегиями.	29 ноября 2021 г.	https://www.zerodayinitiative.com/advisories/ZDI-21-1335/ https://support.kaspersky.com/general/vulnerability.aspx?el=12430#221121	Есть
31	Выполнение произвольных команд в QNAP QVR	MITRE: CVE-2021-38685	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.	29 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021112901 http://www.qnap.com/en/security-advisory/qsa-21-51	Есть
32	Выполнение произвольного кода в ImageMagick	MITRE: CVE-2021-3962	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного ISO-файла. Уязвимость обусловлена ошибкой использования после освобождения.	29 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021112910 http://bugzilla.redhat.com/show_bug.cgi?id=2023196 http://github.com/ImageMagick/ImageMagick/issues/4446 http://github.com/ImageMagick/ImageMagick/commit/82775af03bbb10a0a1d0e15c0156c75673b4525e	Есть
33	Сброс пользовательских паролей в Team Password Manager	MITRE: CVE-2021-44037	Эксплуатация уязвимости позволяет удаленному злоумышленнику сбросить пароль пользователя. Уязвимость обусловлена некорректной работой механизма восстановления пароля.	26 ноября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021112612 http://teampasswordmanager.com/docs/changelog/#10.135.236 http://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-060.txt	Есть