расчетная небанковская кредитная организация

367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б» ОКПО 43340114 БИК № 048209395 корсчет 301038109820900000395

тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 <u>www.psib.ru</u> E-mail: office@psib.ru

«04» апреля 2022г.

г. Махачкала

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за март 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» информационной РНКО (Интернет-банком) служба безопасности «ПРОМСВЯЗЬИНВЕСТ» (OOO)рекомендует it-специалистам (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

<u> [/////</u>Абдурахманов К.А.

Приложение № 1 к информационному письму «Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за март 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.

10	15 3000		La			
№	Наименование уязвимого программного Обеспечения	Идентифи катор уязвимост ей	Описание уязвимости	Дата выявления	Ссылка на источники	Налич ие обнов лений
1.	Уязвимость нулевого дня в CMS Bitrix	ALRT- 20220303.2	Эксплуатация уязвимости позволяет удаленному злоумышленнику записать произвольные файлы в уязвимую систему посредством отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле «vote» CMS Bitrix.	3 марта 2022 г.	-	Есть
2.	Рекомендации по обеспечению безопасности телекоммуникац ионного оборудования	ALRT- 20220305.1	В данных рекомендациях представлены сведения по базовым подходам к о беспечению информационной безопасности телекоммуникационного оборудования (управляемые коммутаторы, маршрутизаторы, межсетевые экраны, далее оборудование), а также его систем управления на участках сопряжения локальных вычислительных сетей предприятий с сетью Интернет, направления на минимизацию рисков проведения компьютерных атак со стороны сети Интернет. 1. Обеспечить изоляцию каналов управления оборудованием и средств управления оборудованием от локально вычислительной сети предприятия. Рекомендуется организовать выделенную (логически изолированную) сеть управления и мониторинга технического состояния, ведения журналов	5 марта 2022 г.	-	Есть
			состояния, ведения журналов событий, аутентификации пользователей. 2. По возможности отключить дистанционное управление оборудованием либо осуществлять такое управление по каналу, защищенному сертифицирова нными ФСБ России средствами криптографической защиты или организационно техническими мерами (выделенный канал), исключающими возможность управления оборудования кем либо кроме администратора. 3. Исключить несанкционированный доступ к управлению оборудовани ем. 4. Создать резервные копии программного обеспечения и			

-						
3.	Уязвимость нулевого дня в Spring Framework	ALRT- 20220331.1	конфигураций оборудования на внешних носителях. Вести учет изменений конфигураций. 5. Ограничть доступ сторонних лиц, привлекаемых к обеспечению технического обслуживания, к системам управления об орудованием. 6. Сменить пароли пользователей и администраторов оборудования и далее проводить такую смену не реже 1 раза в месяц. Устанавливаемые пароли должны соответствовать требованиям «сложности»: - длина пароля должна быть не менее 12 символов; - пароль н е должен основываться на словах естественного языка, а также на том, что связывает его с информацией личностного характера (дата рождения, номер телефона и т.д.); - пароль не должен содержать более 2 следующих друг за другом одинаковых символов, в числе симв олов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.) По каналам Национального координационного центра по компьютерным инцидентам получены сведения об уязвимости «нулевого дня» в одном из популярных фреймворков для разработки Јаvа-приложений - Spring Framework. Обнаруженная уязвимость на данный момент не имеет индентификатора CVE, но носит название Spring4Shell. Указанное	31 марта 2022 г.	https://www.cyberkendra.com/2022/03/spring shell-rce-0-day-vulnerability.html https://bugalert.org/content/notices/2022-03-29-spring.html https://github.com/BobTheShoplifter/Spring4S hell-POC https://www.springcloud.io/post/2022-03/spring-0day-vulnerability/#gsc.tab=0 https://websecured.io/blog/624411cf775ad17 d72274d16/spring4shell-poc	Есть
			информацией личностного			
			характера (дата рождения, номер			
			100000000000000000000000000000000000000			
			пароль не должен содержать более			
		1				
			SELECTION OF THE PROPERTY OF T			
		1	The street of th			
3.	Уязвимость	ALRT-		31 марта	https://www.cyherkendra.com/2022/02/cnring	Fort
	100.00	The Control of the Co		STATE OF THE PARTY OF THE PARTY.	shell-rce-0-day-vulnerability html	LUID
	I					
			1 10		https://github.com/BobTheShoplifter/Spring4S	
				**		
	25		данный момент не имеет			
			The state of the s		3	
		-				
			название присвоено по аналогии с наименованием уязвимости			
			Log4Shell в виду схожести			
			механизма внедрения			
			исполняемого кода. Удаленный			
	20		злоумышленник посредством	S		
			отправки специально			
			сформированных запросов может			
			получить доступ к объекту AccessLogValve, отвечающему за			
			создание журнала доступа к веб-			
			серверу, переопределить			
			параметры логирования и в		* ±	
			последующем направить			
			вредоносный запрос на создание	- 1	Ş	
			JSP-файла, представляющего из себя удаленный исполняемый		`	
			себя удаленный исполняемый файл.			
4.	Выполнение	MITRE:	Эксплуатация уязвимости позволяет	03 июля	https://www.cybersecurity-	Есть
	произвольного	CVE-2017-	удаленному	2017 r.	help.cz/vdb/SB2017070303	-5.0
	кода в Cisco IOS	6736 CVE-	аутентифицированному		http://tools.cisco.com/security/center/content	
	and Cisco IOS XE	2017-6737	злоумышленнику выполнить		/CiscoSecurityAdvisory/cisco-sa-20170629-	
1	l	CVE-2017-	произвольный код в целевой		snmp	1
		6720 015	The state of the s			1 1
	×	6738 CVE-	системе посредством отправки			
		2017-6739	системе посредством отправки специально созданного			
	*	The state of the s	системе посредством отправки			-

		2017-6741 CVE-2017- 6742 CVE- 2017-6743 CVE-2017- 6744	обусловлена некорректной проверкой входных данных.		*1	
5.	Множественные уязвимости в ПО IBM	MITRE: CVE-2021- 41035	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректными доступа.	2022 r.	https://www.cybersecurity-help.cz/vdb/SB2022030806 https://www.cybersecurity-help.cz/vdb/SB2022030803 http://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-sterling-connectdirect-browser-user-interface/http://www.ibm.com/support/pages/node/6561041 http://www.ibm.com/blogs/psirt/security-bulletin-some-unspecified-vulnerabilities-in-java-se-result-in-the-unauthenticated-attacker-to-take-control-of-the-system-or-some-impact/http://www.ibm.com/support/pages/node/6561577	Есть
6.	Множественные уязвимости в ПО IBM	MITRE: CVE-2021- 35560	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	08 марта 2022 г.		Есть
7.	Выполнение произвольных команд ОС в Zyxel NWA1100- NH	MITRE: CVE-2022- 25312	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды ОС в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.	07 марта 2022 г.	http://www.zyxel.com/support/OS-command- injection-vulnerability-of-NWA1100-NH-access- point.shtml https://www.cybersecurity- help.cz/vdb/SB2022030704	Есть
8.	Выполнение произвольного кода в Linux kernel	MITRE: CVE-2022- 25312	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена использованием неинициализированных ресурсов.	08 марта 2022 г.	http://dirtypipe.cm4all.com/ https://www.cybersecurity- help.cz/vdb/SB2022030808	Есть
9.	Выполнение произвольного кода в Microsoft Remote Desktop Client	MITRE: CVE-2022- 21990 CVE- 2022- 23285	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	08 марта 2022 г.	http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022- 21990 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022- 23285 https://www.cybersecurity- help.cz/vdb/SB2022030814	Есть
10.	Выполнение произвольного кода в Adobe Illustrator	MITRE: CVE-2022- 23187	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	09 марта 2022 г.	http://helpx.adobe.com/security/products/illu strator/apsb22-15.html https://www.cybersecurity- help.cz/vdb/SB2022030903	Есть
11.	Выполнение произвольного кода в Microsoft Exchange Server	MITRE: CVE-2022- 23277	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса.	08 марта 2022 г.	http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022- 23277 https://www.cybersecurity- help.cz/vdb/SB2022030818	Есть

			Уязвимость обусловлена некорректной проверкой входных данных.			
12.	Выполнение произвольного кода в Adobe Photoshop	MITRE: CVE-2022- 24090	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	09 марта 2022 г.	http://helpx.adobe.com/security/products/ph otoshop/apsb22-14.html https://www.cybersecurity- help.cz/vdb/SB2022030902	Есть
13.	Множественные уязвимости в Microsoft .NET and Visual Studio	MITRE: CVE-2022- 24512	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	08 марта 2022 г.	https://www.cybersecurity- help.cz/vdb/SB2022030847 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022- 24512 http://msrc.microsoft.com/update- guide/en-US/vulnerability/CVE-2022-24464	Есть
14.	Множественные уязвимости в Microsoft .NET and Visual Studio	MITRE: CVE-2022- 24464	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.	08 марта 2022 г.	https://www.cybersecurity- help.cz/vdb/SB2022030847 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022- 24512 http://msrc.microsoft.com/update- guide/en-US/vulnerability/CVE-2022-24464	Есть
15.	Множественные уязвимости в Mozilla Firefox и Firefox ESR	MITRE: CVE-2022- 26381 CVE- 2022- 26385	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством изменения текста в объекте SVG. Уязвимость обусловлена ошибкой использования после освобождения.	08 марта 2022 г.	https://www.cybersecurity- help.cz/vdb/SB2022030807 http://www.mozilla.org/en- US/security/advisories/mfsa2022-10/ http://www.mozilla.org/en- US/security/advisories/mfsa2022-11/	Есть
16.	Множественные уязвимости в Mozilla Firefox и Firefox ESR	MITRE: CVE-2022- 0843	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	08 марта 2022 г.	https://www.cybersecurity- help.cz/vdb/SB2022030807 http://www.mozilla.org/en- US/security/advisories/mfsa2022-10/ http://www.mozilla.org/en- US/security/advisories/mfsa2022-11/	Есть
17.	Выполнение произвольного кода в Mozilla Firefox	MITRE: CVE-2022- 26485 CVE- 2022- 26486	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. •Уязвимость обусловлена ошибкой использования после освобождения.	05 марта 2022 г.	http://www.mozilla.org/en- US/security/advisories/mfsa2022-09/ https://www.cybersecurity- help.cz/vdb/SB2022030501	Есть
18.	Выполнение произвольного кода в D-Link Router DIR-810L, DIR-820L, DIR- 830L, DIR-826L, DIR-836L	MITRE: CVE-2021- 45382	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	25 февраля 2022 г.	https://github.com/doudoudedi/D- LINK_Command_Injection1/blob/main/D- LINK_Command_injection.md https://supportannouncement.us.dlink.com/an nouncement/publication.aspx?name=SAP1026 4 https://nvd.nist.gov/vuln/detail/CVE-2021- 45382	Есть
19.	Выполнение произвольного кода в D-Link Router DIR-846	MITRE: CVE-2021- 46314	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	25 февраля 2022 г.	https://www.dlink.com/en/security-bulletin/https://github.com/doudoudedi/DIR-846_Command_Injection/blob/main/DIR-846_Command_Injection1.md https://www.tenable.com/cve/CVE-2021-46314 https://www.opencve.io/cve/CVE-2021-46314	8
20.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022- 0800	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством	04 марта 2022 г.	http://crbug.com/1294097 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-0794 http://chromereleases.googleblog.com/2022/0	Есть

21. Миожественные украимости в МПТВ: 202-202-2036 Мистовет в				T			
Concention Co						3/stable-channel-update-for-desktop.html	
1				специально созданной вредоносной		http://crbug.com/1282782	
1. Миожественные узавимости в Мітве: 2022-0903 (VE-2022-0904 сустем в						http://portal.msrc.microsoft.com/en-	
1.3 http://chromereleases_googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://chromereleases_googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://chromereleases_googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://chromereleases_googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/125978 http://chromereleases_googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1259786 http://c				обусловлена ошибкой границ		US/security-guidance/advisory/CVE-2022 0705	
3/stable-channel-update-for-desktop.html http://chup.com/128198 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0795 http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.html http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.html http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.html http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.html http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.html http://chug.com/1281987 http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.html http://chug.com/1281987 http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.html http://chumoreleases.googlebiog.com/2022/0 3/stable-channel-update-for-desktop.						http://chromereleases.googlobleg.com/2022/0	
1. Мижественные узавимости в повьюдателем повьюдателем провретиой предостать обусповлена в дооре с hrome 1. 1. 1. 1. 1. 1. 1. 1				and the state of t		3/stable shannel undets for delice to the	1
21. Множественные учазимости а Міствогі Ебде Подравник проверок безопасности. Подравня проверок подравня проверок подравня проверок подравня проверок проверок предест подволя проверсок подравня процести в подравня проверок подравня прове						bttm://ark.com/dagate-for-desktop.html	1
2.1. Мисмественные увазмисти в водове с мограти подволяет удаленному выпости в водове с мограти подволяет и удаленному выпостить произвольной код в водове с мограти подволяет и удаленному выпостить произвольной код в водове с мограти подволяет и и и и и и и и и и и и и и и и и и и						nttp://crbug.com/1295/86	
1. 1. 1. 1. 1. 1. 1. 1.						nttp://portal.msrc.microsoft.com/en-	
3/stable-channel-update-for-desktop.html http://crbug.com/pata-for-desktop.html http://crbug.						US/security-guidance/advisory/CVE-2022-0796	
1. Множественные ухавимости о в Міггозоft Edge						http://chromereleases.googleblog.com/2022/0	
Minomecraentuse						3/stable-channel-update-for-desktop.html	
21. Множественные мігке: указымости в містової t Edge містової пользователем містової t Edge містової t Edg						http://crbug.com/1281908	
21. Множественные мітке: указымости в містозоft Edge містозоft Ed						http://portal.msrc.microsoft.com/en-	
21. Множественные узвимости в Мітве: обусловна узвимости позволяет удаленному значимости позволяет удаленному стача по предоставленници по предоставленни по предоставленни по предоставленним по предоставленни по предоставленни по пре				⊕ .		US/security-guidance/advisory/CVE-2022-0797	
21. Множественные уязвимости в Мігке: 1202-2-20-20-20-20-20-20-20-20-20-20-20-2						http://chromereleases.googleblog.com/2022/0	
21. Множественные узавимости в містовогі є є сує-2022- о воз сує-2022- о в в сує-2022- о						3/stable-channel-update-for-deskton html	
4.1. Множественные уэзмимости в иденей костом (стеменей узмимости в разменному испорчить НСД к целевой системе подредством подамной предоносной в беб-страницы. Узявимости озволяет удаленному злоумышленнику узвимости озволяетем специально созданной вредоносной в беб-страницы. Узявимосты в Google Chrome МПТКЕ: Обественные узмимости в подволяет идаленному злоумышленнику замимости позволяет и пользователем специально созданной вредоносной в беб-страницы. Узявимосты в Google Chrome МПТКЕ: Обественные узмимости в подволяет идаленному злоумышленнику замимости подволяет и пользователем специально созданной вредоносной веб-страницы. Узявимость обусловлена ошибкой границ памити. Эмсплуатация узявимости подволяет удаленному злоумышленнику значное посредством открытия пользователем специально созданной вредоносной веб-страницы. Узявимость обусловлена ошибкой границ памити. Эмсплуатация узявимости подволяет удаленному злоумышленнику							
Wassemmocru в CVE-2022- 2022-8080 CVE- 2022-8080 CVE- 2	21.	Множественные	MITRE:	Эксплуатация уязвимости позволяет	04 марта		
Microsoft Edge		уязвимости в	CVE-2022-	And the second s	A PROPERTY OF THE PARTY OF THE	http://nortal.mara.mia.a.a.f	Есть
2022-0802 ОСК-2022-0803 ССК-2022-0803 ССК-2022-0807 ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ УЯЗВИМОСТЬ ООЗДАНОЙ ВРЕДОНОСНОЙ В ОБЕСТРАНИЦЫ УЯЗВИМОСТЬ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ УЯЗВИМОСТЬ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ УЯЗВИМОСТЬ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ УЯЗВИМОСТЬ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ УЯЗВИМОСТЬ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦЫ ООЗДАНОЙ ВРЕДОНОСНОЙ ВЕСТРАНИЦИИ ВЕСТРАНИИ ВЕСТ		Microsoft Edge	0801 CVE-		20221.	115 / conviction of the conference of the confer	
22. Множественные узвымости в Google Chrome МПТЕ: Оказанной провором безопасности. Эксплуатация узазимости позволяет обусловлены невой открытия произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Узазимость обусловлена некорректной реализацией провером безопасности. Финар обусловлена ошибкой границ памяти. Фудаленному злоумышлениих работой процесса в обусловлена некоректной работой праводнения узаимость обусловлена некоректной работой процесса в обусловлена некоректной работой пработой процесса в обусловлена некоректной работой процесса в обусловлена некоректной процесса в обусловлена некоректной процесса в обусловлена некоректном подклага некоректном подклага			The state of the same of the s			Us/security-guidance/advisory/CVE-2022-0794	
8803 CVE- 2022-0804			The second second second second	The second secon	1	http://chromereleases.googleblog.com/2022/0	
2022-0804 CVE-2022-0807 2027-0807 2027-0807 2028-0807 2028-0807 2028-0807 2028-0807 2028-0807 2028-0807 2028-0807 2029-0808 2039-0808 2049-08				I consider the second s		3/stable-channel-update-for-desktop.html	
CVE-2022- 0807 проверок безопасности. Security-guidance/advisory/CVE-2022-0795 http://cromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://crbug.com/2195786 http://cr			AND THE PROPERTY OF THE PARTY O				
With the content of the position of the pos	1			122		http://portal.msrc.microsoft.com/en-	
No.			The state of the s			US/security-guidance/advisory/CVE-2022-0795	
3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://portal.msrc.microsoft.com/en-U5/security-guidance/advisory/CVE-2022-0796 http://chomereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://portal.msrc.microsoft.com/en-U5/security-guidance/advisory/CVE-2022-0797 http://crbug.com/1281908 http://portal.msrc.microsoft.com/en-U5/security-guidance/advisory/CVE-2022-0797 http://crbug.com/1289383 http://crbug.com/128782 http://portal.msrc.microsoft.com/en-U5/security-guidance/advisory/CVE-2022-0794 http://crbug.com/128782 http://portal.msrc.microsoft.com/en-U5/security-guidance/advisory/CVE-2022-0794 http://crbug.com/1282782 http://portal.msrc.microsoft.com/en-U5/security-guidance/advisory/CVE-2022-0795 http://crbug.com/1282782 http://portal.msrc.microsoft.com/en-U5/security-guidance/advisory/CVE-2022-0796 http://crbug.com/1281908 http://c	1		0807	проверок безопасности.	1	http://chromereleases.googleblog.com/2022/0	
http://crbug.com/1295786 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0797 http://crbmereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1283933 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0797 http://crbmereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbmereleases.googleblog.com/2022/0 3/st						3/stable-channel-update-for-deskton html	1 1
### http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://bortal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-0797 http://crbug.com/1282908 http://crbug.com/1282908 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/12829383 http://crbug.com/12829383 O4 марта 2022 г. 0800 Висплуатация уязвимость позволяет удаленному злоумышленнику выполныть произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена памяти. Уязвимость обусловлена памяти. Витир//crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/128308 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/128308 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.						http://crbug.com/1295786	1
22. Множественные уязвимости в Google Chrome 0800						http://portal mars microsoft as m/an	1
Action						IIS/security guidence/eduice/SVE 2022 0725	1
22. Множественные уязвимости в Google Chrome Google Chrom						bttm://abrana and an and a series and a seri	1 1
A						nttp://chromereleases.googleblog.com/2022/0	1 1
MITRE:							1
22. Множественные уязвимости в Google Chrome MITRE: Удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 23. НСД в several Zyxel firewalls WITRE: VGE-2022-0342 MITRE: Ожеглуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Позволяет удаленному злоумышленнику получить НСД к целевой системе. Позволяет удаленному злоумышленнику получить НСД к целевой системе. Обусловлена некорректной работой процесса US/security-guidance/advisory/CVE-2022-0794 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/12821908 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/12821908 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http							
22. Множественные уязвимости в Google Chrome МITRE: Овоо вооружения выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. В ССТ-2022- Овоо в него в выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. В ССТ-2012- Овоо в него в пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. В ССТ-2012- Овоо в него в пользователем специально созданной вредоносной в веб-страницы. Уязвимость обусловлена ошибкой границ памяти. В ССТ-2012- Овоо в него в пользователем специально созданной вредоносной в веб-страницы. Уязвимость обусловлена в пользователем специально созданной вредоносной в веб-страницы. Овоо в пользователем специально созданной вредоносной в веб-страницы. Овоо в пользователем специально созданной вредоносной в веб-страницы. Овоо в пользователем специально созданной вредоносной в пользователем специально созданной вредоносной в веб-страницы. Овоо в пользователем специально созданной в пользователем специально стеме. Обусловлена некорректной процесса обусловлена некорректной позволяет учить некорректной позволяет стемена обусловлена некорректной позволяет учить некорректной позволяет учить некорректной позволяет стемена обусловная некорректной позволяет учить некорректной п						http://portal.msrc.microsoft.com/en-	
22. Множественные уязвимости в Google Chrome MITRE: CVE-2022- 0800 Выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 23. НСД в several Zyxel firewalls MITRE: CVE-2022- 0342 MITRE: CVE-2022- 0800 МITRE: CVE-2022- 0800 Висплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса						US/security-guidance/advisory/CVE-2022-0797	
22. Множественные уязвимости в Google Chrome MITRE: CVE-2022- 0800 Выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 23. НСД в several Zyxel firewalls MITRE: CVE-2022- 0342 MITRE: CVE-2022- 0800 МITRE: CVE-2022- 0800 Висплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Висплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса						http://chromereleases.googleblog.com/2022/0	
MHожественные уязвимости в Google ChromeMITRE: ОКЕ-2022- 0800Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.04 марта 2022 г.http://crbug.com/1289383ECTЬ23.HCД в several Zyxel firewallsMITRE: CVE-2022- 0342Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса30 марта 2022 г.http://crbug.com/12893834http://crbug.com/1289383http://crbug.com/12893836http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0794 http://crbug.com/1282782 http://crbug.com/1282782 http://crbug.com/1282782 http://crbug.com/1282782 http://crbug.com/1282782 http://crbug.com/1282782 http://crbug.com/1282983						3/stable-channel-update-for-desktop.html	
22.Множественные уязвимости в Google ChromeОКЕ-2022- 0800Эксплуатация уязвимости поризвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.04 марта удаленному выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.04 марта (http://crbug.com/1294097 (http://portal.msrc.microsoft.com/en-uS/security-guidance/advisory/CVE-2022-0794 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1292763 (systable-channel-update-for-desktop.html http://crbug.com/1295786 (http://crbug.com/1295786 (http://crbug.com/1295786 (http://crbug.com/1295786 (http://crbug.com/1295786 (http://crbug.com/129181908 (http://crbug.com/1281908 (http://crbug.com/1281908 (http://crbug.com/1281908 (http://crbug.com/1282782 (http://crbug.com/1294097 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1294097 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1294097 (http://crbug.com/1282782 (http://crbug.com/1294097 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1294097 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/129270 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1294097 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1294097 (http://crbug.com/1282782 (http://crbug.com/1282782 (http://crbug.com/1282782	200					http://crbug.com/1289383	
удаленному элоумышленнику выполнить произвольной код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 23. НСД в several Zyxel firewalls WITRE: CVE-2022- 0342 VДаленному элоумышленнику выполнить произвольной код в целевой системем посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. VЯЗВИМОСТЬ ОКОТЕ-2022 г. http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786	22.	Множественные	MITRE:	Эксплуатация уязвимости позволяет	04 марта		Ecz
US/security-guidance/advisory/CVE-2022-0794 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://crbug.com/1295786 http://crbug.com/1295786 http://crbug.com/1295786 http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://crbug.com/1295			CVE-2022-	удаленному злоумышленнику	2022 г.		LCIB
целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. Територия открытия пользователем оподадиность обусловлена памяти. Нестраницы. Уязвимость обусловлена пользователем обусловлена некорректной работой процесса Втема открытия пользователем открытия пользователем открытия пользователем открытия пользователем открытия пользователем обусловлена некорректной работой процесса Нестраницы. Уязвимость обусловлена некорректной работой процесса Втема открытия пользователем открытительный откр		Google Chrome	0800	выполнить произвольной код в	No. of Control of Cont	US/security-guidance/advison/CVE 2022 0704	
открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 23. НСД в several Zyxel firewalls WITRE: OTKPЫТИЯ OTKPЫТИЯ ПОЛЬЗОВАТЕЛЬНОЕ В SEVERAL ZYXEL FIREWALLS OTKPЫТИЯ OTKPЫТИЯ ПОЛЬЗОВАТЕЛЬНОЕ В SEVERAL ZYXEL FIREWALLS OTKPЫТИЯ ОТКРЫТИЯ ОТКРИТИЯ ОТКРЫТИЯ ОТКРЫТИЯ ОТКРЫТИЯ ОТКРИТИЯ ОТКРЫТИЯ ОТКРЫТИЯ						http://shromorologges.googleble/2022/0	
специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти. 23. НСД в several Zyxel firewalls WITRE: CVE-2022- 0342 МITRE: Уязвимость обусловлена уязвимости позволяет дуязвимость обусловлена некорректной работой процесса Оправления и веб-страницы. Уязвимость обусловлена некорректной работой процесса Нttp://crbug.com/1282782 http://crbug.com/1282782 http://crbug.com/1295786 http://crbug.c						2/stable shared walks for the territory	
веб-страницы. Уязвимость обусловлена ошибкой границ памяти. Веб-страницы. Уязвимость обусловлена ошибкой границ памяти. Веб-страницы. Уязвимость обусловлена ошибкой границ памяти. Веб-страницы. Уязвимость обусловлена некорректной работой процесса Нttp://cprtal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0795 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 ВЕО-СТВ НТД В SEVERAL ZAVEL SEVERAL ZAV						bttm://mlanner-update-for-desktop.html	
обусловлена ошибкой границ памяти. US/security-guidance/advisory/CVE-2022-0795 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 HCД в several Zyxel firewalls WITRE: CVE-2022-0342 Обусловлена ошибкой границ US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 HCД в several Zyxel firewalls Обусловлена ошибкой границ US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 НСД в several Zyxel firewalls Обусловлена ошибкой границ US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 В ксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса Обусловлена ошибкой границ ИЗ/security-дидане-for-desktop.html http://crbug.com/1281908 В ксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса			2			nttp://crbug.com/1282782	
ламяти. http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 PKCII B several Zyxel firewalls MITRE: CVE-2022- 0342 MITRE: CVE-2022- 0342 MITRE: CVE-2022- 0342 AMITRE: CVE-2022- 0342 MITRE: CVE-2022- 0342 AMITRE: 2022 г. MITRE: 2022 г. AMITRE: 2022 г. AMITRE: 2022 г. AMITRE: 2022 г. WITRE: 2022 г. AMITRE: 2022 г.			美丰二			http://portal.msrc.microsoft.com/en-	
3/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://crbug.com/cve-zo22-0796 http://chromereleases.googleblog.com/z022/0 3/stable-channel-update-for-desktop.html http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 ВКСПЛУАТАЦИЯ УЯЗВИМОСТИ ПОЗВОЛЯЕТ Zyxel firewalls ВКСПЛУАТАЦИЯ УЯЗВИМОСТИ ПОЗВОЛЯЕТ Zyxel firewalls ОКЕ-2022-0342 ОЗИВИТЕ: ОКЕ-2022-0342 ОЗИ						US/security-guidance/advisory/CVE-2022-0795	
http://crbug.com/1295786 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 Вксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса http://crbug.com/1295786 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-03/3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908				памяти.		http://chromereleases.googleblog.com/2022/0	
http://crbug.com/1295786 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 Вксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса http://crbug.com/1295786 http://portal.msrc.microsoft.com/en- US/security-guidance/advisory/CVE-2022-03/3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1281908 http://crbug.com/1295786 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908						3/stable-channel-update-for-desktop.html	1
23. HCД в several Zyxel firewalls WITRE: CVE-2022- 0342 DUS/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1281908 http://www.zyxel.com/support/Zyxel-security-advisory-for-authentication-bypass-vulnerability-of-firewalls.shtml ECTЬ VЯЗВИМОСТЬ ОБУСЛОВЛЕНА НЕКОРРЕКТНОЙ работой процесса							
23. HCД в several Zyxel firewalls WITRE: CVE-2022- 0342 DUS/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1281908 http://www.zyxel.com/support/Zyxel-security-advisory-for-authentication-bypass-vulnerability-of-firewalls.shtml ECTЬ VЯЗВИМОСТЬ ОБУСЛОВЛЕНА НЕКОРРЕКТНОЙ работой процесса				i			
23. HCД в several Zyxel firewalls CVE-2022- 0342 МІТВЕ: Уязвимость обусловлена некорректной работой процесса http://chromereleases.googleblog.com/2022/0 3/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://crbug.com/1281908						US/security-guidance/advisory/CVF-2022-0796	
3/stable-channel-update-for-desktop.html http://crbug.com/1281908 НСД в several Zyxel firewalls CVE-2022- 0342 Яндери обусловлена некорректной работой процесса Яндери обуслования о						http://chromereleases.googleblog.com/2022/0	
23. HCД в several Zyxel firewalls CVE-2022- 0342						3/stable-channel-undate-for-dockton basel	
23. HCД в several Zyxel firewalls CVE-2022- 0342						http://crhug.com/1201000	
Zyxel firewalls CVE-2022- 0342 VAJAЛЕННОМУ ЗЛОУМЫШЛЕННИКУ ПОЛУЧИТЬ НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса ОТЕ-2022-	23.	НСД в several	MITRE:	Эксплуатация уязвимости позволяет	30	http://croug.com/1281908	
0342 получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса						nttp://www.zyxel.com/support/Zyxel-security-	Есть
Уязвимость обусловлена некорректной работой процесса		_,	A STATE OF THE PROPERTY OF THE		2022 F.		
некорректной работой процесса			0372			vulnerability-of-firewalls.shtml	
				The state of the s			
аутентификации.			1				
			,	аутентификации.			