

## **Задание:**

Установите сканер уязвимостей и выполните следующие задачи:

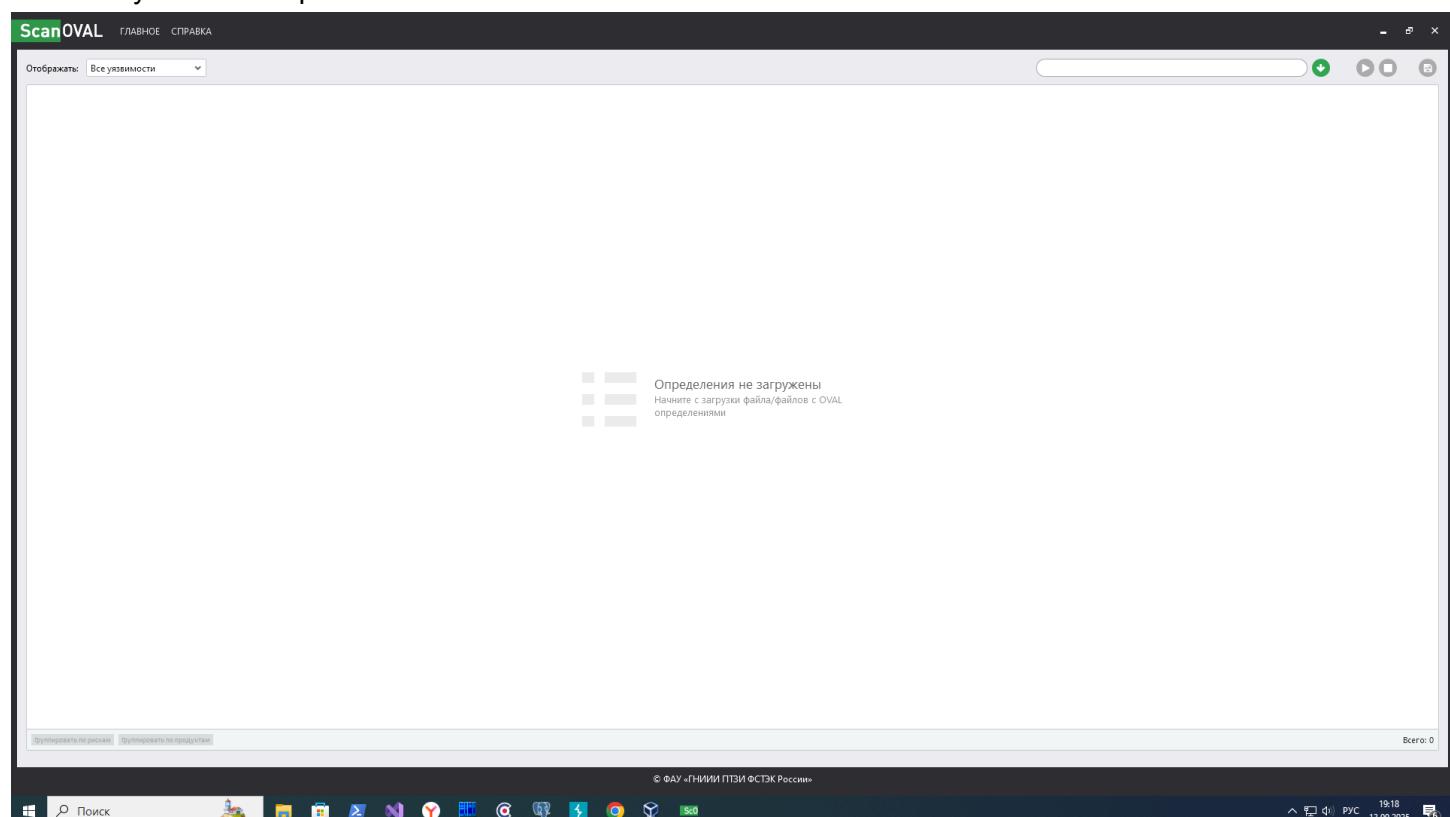
1. Проведите сканирование хоста или сети на наличие уязвимостей.
2. Проанализируйте любую критическую уязвимость. Если критическая уязвимость отсутствует, то возьмите следующую по критичности.

Проанализируйте уязвимость на эти критерии:

- Что уязвимо?
  - Как может быть реализована уязвимость?
  - Прочитать описание на CVE?
  - Как устранить уязвимость?
3. Устранитте уязвимости.
  4. Проведите повторное сканирование.

Я буду использовать сканер ScanOVAL.

Запускаю сканер ScanOVAL:



Загружаю базу OVAL определений

ScanOVAL			
ГЛАВНОЕ СПРАВКА			
Отображать: Все уязвимости			
Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники
BDU-2015-10240	<span>Критический</span>		VULN-20211124; active-saltstack
BDU-2021-06345	<span>Критический</span>		Уязвимость системы управления базами данных Линтер Бастон, позволяющая злоумышленнику выполнить произвольный код с правами системы (BDU-2015-10240)
BDU-2023-06017	<span>Критический</span>		Уязвимость внедрения команд в rirk пакет salt до 3002.5 и до 3001.6 и до 3000.8 (active-saltstack-cve-release-2021-feb-25)
BDU-2021-04041	<span>Критический</span>		CVE-2023-5074
BDU-2023-06077	<span>Критический</span>		Уязвимость в D-Link D-View 8 до 2.0.2.89 (BDU-2023-06017)
BDU-2020-02500	<span>Критический</span>		mfsa2016-86; mfsa2016-88; CVE-2C
BDU-2020-02500	<span>Критический</span>		Уязвимость доступа к свободной памяти в Mozilla Firefox до 49.0 и Firefox ESR 45.x до 45.4 (mfsa2016-86, mfsa2016-88, mfsa2016-85)
BDU-2016-02178	<span>Критический</span>		VULN-20200513-14; CVE-2020-090*
BDU-2022-01702	<span>Критический</span>		Уязвимость удаленного выполнения кода в Microsoft Excel (BDU-2020-02500)
BDU-2023-08257	<span>Критический</span>		Уязвимость в Pepper Flash до 18.0.0.375 в 19.x и до 23.x до 23.0.0.162 (apib16-29)
BDU-2015-12022	<span>Критический</span>		Nessus Vulnerability Scanner до 8.15.4 и до 10.0.0 до 10.1.2, Nessus Network Monitor до 6.2.0 (Nessus, Nessus)
BDU-2022-02541	<span>Критический</span>		CVE-2015-7665; apib15-28
BDU-2015-11675	<span>Критический</span>		Уязвимость в Docker Desktop до 4.2.3.0 (BDU-2023-06077)
BDU-2022-02547	<span>Критический</span>		Уязвимость доступа к свободной памяти в Mozilla Firefox до 49.0 и Firefox ESR 45.x до 45.4 (mfsa2016-86, mfsa2016-88, mfsa2016-85)
BDU-2023-06465	<span>Критический</span>		Уязвимость в GStreamer до 1.2.2.7 (BDU-2023-08257)
BDU-2015-09525	<span>Критический</span>		Уязвимость в Apache Cyber Protect до build 35979 (BDU-2023-06465)
BDU-2023-06603	<span>Критический</span>		opennsi-dos.txt; 4773; CVE-2006-4
BDU-2016-01366	<span>Критический</span>		CVE-2023-4149
BDU-2016-00270	<span>Критический</span>		Уязвимость в rirk пакете gevent до 23.9.0 (BDU-2023-06002)
BDU-2015-07655	<span>Критический</span>		Уязвимость доступа к свободной памяти в Google Chrome до 47.0.2526.73 (stable-channel-update)
BDU-2024-00321	<span>Критический</span>		CVE-2024-22051; GHSA-fm4x-26f3
BDU-2015-12230	<span>Критический</span>		Уязвимость в commonmarker.js до 0.23.4 (GHSA-fm4x-26f3-wqpf, commonmarker)
BDU-2022-02555	<span>Критический</span>		Уязвимость в Adobe Flash Player до 18.0.0.268 и 19.x и 20.x до 20.0.0.228, Adobe AIR до 20.0.0.204 (apib15-32)
BDU-2015-09596	<span>Критический</span>		Перенесение стека в PHP до 5.5.32, 5.6.x до 5.6.18, и 7.x до 7.0.3 (PHP_7_0, PHP_5_5, PHP_5_6)
BDU-2024-05906	<span>Критический</span>		VULN-20240728.15; CVE-2024-7-23
BDU-2016-01366	<span>Критический</span>		Уязвимость в PHP до 5.4.40, 5.5.x до 5.5.4, и 5.6.x до 5.6.8 (PHP_5_6, PHP_5_5, PHP_5_4)
BDU-2016-02310	<span>Критический</span>		CVE-2016-6941; apib16-33
BDU-2016-01369	<span>Критический</span>		Уязвимость в Adobe Reader и Acrobat до 11.0.18, Acrobat и Acrobat Reader DC Classic до 15.006.30243, и Acrobat и Acrobat Reader DC Continuous до 15.020.20039 (apib16-33)
BDU-2016-02309	<span>Критический</span>		Уязвимость в PHP до 5.4.40, 5.5.x до 5.5.24, и 5.6.x до 5.6.8 (PHP_5_6, PHP_5_5, PHP_5_4)
BDU-2016-02292	<span>Критический</span>		Уязвимость в Adobe Reader и Acrobat и Acrobat и Acrobat Reader DC Classic до 15.006.30243, и Acrobat и Acrobat Reader DC Continuous до 15.020.20039 (apib16-33)
BDU-2017-00034; BDU-2017-0002	<span>Критический</span>		CVE-2016-7875; apib16-39
BDU-2017-00027; BDU-2016-0238	<span>Критический</span>		Уязвимость в Pepper Flash 23.0.0.207 и ниже (apib16-39)
BDU-2017-00027; BDU-2016-0238	<span>Критический</span>		Уязвимость в Adobe Flash Player 23.0.0.207 и ниже (apib16-39)
BDU-2021-04796	<span>Критический</span>		VULN-20210914.1; VULN-20210917
BDU-2025-03316	<span>Критический</span>		Уязвимость доступа к предзаписи памяти в Node.js пакете electron до 13.5.0 и до 12.2.0 (electron)
BDU-2016-00543	<span>Критический</span>		Microsoft Edge (BDU-2025-03316)
BDU-2021-04999	<span>Критический</span>		openshift/origin; CVE-2016-906;
BDU-2021-11001; Chrome-VB-Log	<span>Критический</span>		Уязвимость в openshift/origin до 1.1.0 (openshift/origin, GHSA-m3fm-h5jp-q79p)
BDU-2021-05503	<span>Критический</span>		VULN-20211102.3; CVE-2021-3799
BDU-2021-05969	<span>Критический</span>		Уязвимость доступа к свободной памяти в Google Chrome до 14.1.1 и до 13.5.2 и до 12.2.2 (Chrome-VB-Logic-Bug-Use-After-Free, electron)
BDU-2025-02676	<span>Критический</span>		opennsi-dos.txt; 4773; CVE-2006-4
BDU-2025-02676	<span>Критический</span>		Уязвимость в VMware vCenter Server 6.7 и 6.5 (VMware-vCenter-Server-Unauthorized-Log4Shell-JNDI-Injection-Remote-Code-Execution, UniFi-Network-Application-Unauthenticated-Log4Shell-Remote-Code-...
BDU-2015-11890	<span>Критический</span>		VMware-vCenter-Server-Unauthorized-Log4Shell-JNDI-Injection-Remote-Code-Execution, Log4Shell-HTTP-Header-Injection, UniFi-Network-Application-Unauthenticated-Log4Shell-Remote-Code-...
Напоминаем о важности в Осторожность! А также Java SE Kit10, 7u85, и 8u60 (см. #2015-2367957).			
Проверка по рискам Проверка по продуктам			
2 файла(ов) загружено.			
Всего: 32252			

© ФАУ «ГНИИ ПТЗ ФСТЭК России»

ПОИСК ВЫБОРЫ СПРАВКА 19:21 13.09.2025

## Запускаю сканирование хостовой машины с помощью ScanOVAL

ScanOVAL			
ГЛАВНОЕ СПРАВКА			
Отображать: Все уязвимости			
Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники
BDU-2015-10240	<span>Критический</span>		VULN-20211124; active-saltstack
BDU-2021-06345	<span>Критический</span>		Уязвимость системы управления базами данных Линтер Бастон, позволяющая злоумышленнику выполнить произвольный код с правами системы (BDU-2015-10240)
BDU-2023-06017	<span>Критический</span>		Уязвимость внедрения команд в rirk пакет salt до 3002.5 и до 3001.6 и до 3000.8 (active-saltstack-cve-release-2021-feb-25)
BDU-2021-04041	<span>Критический</span>		CVE-2023-5074
BDU-2023-06077	<span>Критический</span>		Уязвимость в D-Link D-View 8 до 2.0.2.89 (BDU-2023-06017)
BDU-2020-02500	<span>Критический</span>		mfsa2016-86; mfsa2016-88; CVE-2C
BDU-2020-02500	<span>Критический</span>		Уязвимость доступа к свободной памяти в Mozilla Firefox до 49.0 и Firefox ESR 45.x до 45.4 (mfsa2016-86, mfsa2016-88, mfsa2016-85)
BDU-2016-02178	<span>Критический</span>		VULN-20200513-14; CVE-2020-090*
BDU-2022-01702	<span>Критический</span>		Уязвимость удаленного выполнения кода в Microsoft Excel (BDU-2020-02500)
BDU-2023-08257	<span>Критический</span>		Уязвимость в Pepper Flash до 18.0.0.375 в 19.x и до 23.x до 23.0.0.162 (apib16-29)
BDU-2015-12022	<span>Критический</span>		Nessus Vulnerability Scanner до 8.15.4 и до 10.0.0 до 10.1.2, Nessus Network Monitor до 6.2.0 (Nessus, Nessus)
BDU-2022-02541	<span>Критический</span>		CVE-2015-7665; apib15-28
BDU-2015-11675	<span>Критический</span>		Уязвимость в Docker Desktop до 4.2.3.0 (BDU-2023-06077)
BDU-2022-02547	<span>Критический</span>		Уязвимость доступа к свободной памяти в Mozilla Firefox до 49.0 и Firefox ESR 45.x до 45.4 (mfsa2016-86, mfsa2016-88, mfsa2016-85)
BDU-2023-06465	<span>Критический</span>		Целочисленное переполнение в PHP до 5.5.37 и 5.6.x до 5.6.2 (PHP_5_5, PHP_5_6)
BDU-2015-09525	<span>Критический</span>		Целочисленное переполнение в PHP до 5.5.36 и 5.6.x до 5.6.2 (PHP_5_5, PHP_5_6)
BDU-2023-06603	<span>Критический</span>		Уязвимость в Apache Cyber Protect до build 35979 (BDU-2023-06465)
BDU-2016-01366	<span>Критический</span>		opennsi-dos.txt; 4773; CVE-2006-4
BDU-2016-00270	<span>Критический</span>		CVE-2023-4149
BDU-2016-02292	<span>Критический</span>		Уязвимость доступа к свободной памяти в Google Chrome до 47.0.2526.73 (stable-channel-update)
BDU-2024-00321	<span>Критический</span>		CVE-2024-22051; GHSA-fm4x-26f3
BDU-2015-12230	<span>Критический</span>		Уязвимость в commonmarker.js до 0.23.4 (GHSA-fm4x-26f3-wqpf, commonmarker)
BDU-2022-02555	<span>Критический</span>		Уязвимость в Adobe Flash Player до 18.0.0.268 и 19.x и 20.x до 20.0.0.228, Adobe AIR до 20.0.0.204 (apib15-32)
BDU-2015-09596	<span>Критический</span>		Перенесение стека в PHP до 5.5.32, 5.6.x до 5.6.18, и 7.x до 7.0.3 (PHP_7_0, PHP_5_5, PHP_5_6)
BDU-2024-05906	<span>Критический</span>		VULN-20240728.15; CVE-2024-7-23
BDU-2016-01366	<span>Критический</span>		Уязвимость в PHP до 5.4.40, 5.5.x до 5.5.24, и 5.6.x до 5.6.8 (PHP_5_6, PHP_5_5, PHP_5_4)
BDU-2016-02310	<span>Критический</span>		CVE-2016-6941; apib16-33
BDU-2016-01369	<span>Критический</span>		Уязвимость в Adobe Reader и Acrobat до 11.0.18, Acrobat и Acrobat Reader DC Classic до 15.006.30243, и Acrobat и Acrobat Reader DC Continuous до 15.020.20039 (apib16-33)
BDU-2016-02309	<span>Критический</span>		Уязвимость в PHP до 5.4.40, 5.5.x до 5.5.24, и 5.6.x до 5.6.8 (PHP_5_6, PHP_5_5, PHP_5_4)
BDU-2016-02292	<span>Критический</span>		Уязвимость в Adobe Reader и Acrobat и Acrobat и Acrobat Reader DC Classic до 15.006.30243, и Acrobat и Acrobat Reader DC Continuous до 15.020.20039 (apib16-33)
BDU-2017-00034; BDU-2017-0002	<span>Критический</span>		CVE-2016-7875; apib16-39
BDU-2017-00027; BDU-2016-0238	<span>Критический</span>		Уязвимость в Pepper Flash 23.0.0.207 и ниже (apib16-39)
BDU-2017-00027; BDU-2016-0238	<span>Критический</span>		Уязвимость в Adobe Flash Player 23.0.0.207 и ниже (apib16-39)
BDU-2021-04796	<span>Критический</span>		VULN-20210914.1; VULN-20210917
BDU-2025-03316	<span>Критический</span>		Уязвимость доступа к предзаписи памяти в Node.js пакете electron до 13.5.0 и до 12.2.0 (electron)
BDU-2016-00543	<span>Критический</span>		Microsoft Edge (BDU-2025-03316)
BDU-2021-04999	<span>Критический</span>		openshift/origin; CVE-2016-906;
BDU-2021-04999	<span>Критический</span>		Уязвимость доступа к свободной памяти в Node.js пакете electron до 14.1.1 и до 13.5.2 и до 12.2.2 (Chrome-VB-Logic-Bug-Use-After-Free, electron)
BDU-2021-04999	<span>Критический</span>		VULN-20211101.3; Chrome-VB-Log
BDU-2021-05503	<span>Критический</span>		Уязвимость доступа к свободной памяти в Node.js пакете electron до 14.2.1 и до 13.6.2 и до 12.2.3 (electron)
BDU-2021-05969	<span>Критический</span>		Уязвимость выполнения произвольного кода в Ruby gem log4j-jars since 2.0.0rc1 (VMware-vCenter-Server-Unauthenticated-Log4Shell-JNDI-Injection-Remote-Code-Execution, UniFi-Network-Application-Unauthenticated-Log4Shell-Remote-Code-...
BDU-2025-02676	<span>Критический</span>		VMware-vCenter-Server-Unauthorized-Log4Shell-JNDI-Injection-Remote-Code-Execution, Log4Shell-HTTP-Header-Injection, UniFi-Network-Application-Unauthenticated-Log4Shell-Remote-Code-...
BDU-2015-11890	<span>Критический</span>		VMware-vCenter-Server-Unauthorized-Log4Shell-JNDI-Injection-Remote-Code-Execution, Log4Shell-HTTP-Header-Injection, UniFi-Network-Application-Unauthenticated-Log4Shell-Remote-Code-...
Напоминаем о важности в Осторожность! А также Java SE Kit10, 7u85, и 8u60 (см. #2015-2367957).			
Проверка по рискам Проверка по продуктам			
2 файла(ов) загружено.			
Всего: 32252			

© ФАУ «ГНИИ ПТЗ ФСТЭК России»

ПОИСК ВЫБОРЫ СПРАВКА 19:25 13.09.2025

ScanOVAL		ГЛАВНОЕ СПРАВКА	
Обображені:		Только обнаруженные	
Идентификатор уязвимости	Результат	Уровень	Ссылки на источники
BUU-2025-09829	Обнаружено	Критический	CVE-2025-8714; 3118
BUU-2025-00318	Обнаружено	Критический	VULN-20250117.73; CVE-2025-21273; CVE-2025-21273
BUU-2025-02676	Обнаружено	Критический	VULN-20250117.81; Chr-2025-3-4; CVE-2025-1919
BUU-2025-02762	Обнаружено	Критический	CVE-2025-24095; CVE-2025-24056
BUU-2022-07403	Обнаружено	Критический	CVE-2022-32232; CVE-2022-32221
BUU-2025-04921	Обнаружено	Критический	VULN-20250425.9; VULN-20250430.5; Chr-2025-4-15; CVE-2025-3620
BUU-2025-00436	Обнаружено	Критический	VULN-20250117.72; CVE-2025-21252; CVE-2025-21252
BUU-2025-10156	Обнаружено	Критический	Chr-2025-8-12; CVE-2025-8880
BUU-2025-00286	Обнаружено	Критический	VULN-20250117.83; CVE-2025-21233; CVE-2025-21233
BUU-2020-05719	Обнаружено	Критический	CVE-2020-0683; apib20-45
BUU-2025-04103	Обнаружено	Критический	CVE-2025-27477; CVE-2025-27477
BUU-2024-02124	Обнаружено	Критический	CVE-2024-21440; CVE-2024-21440
BUU-2025-04118	Обнаружено	Критический	CVE-2025-21221; CVE-2025-21221
BUU-2020-01217	Обнаружено	Критический	VULN-20200319.10; CVE-2020-3775; apib20-14
BUU-2020-01223	Обнаружено	Критический	VULN-20200319.10; CVE-2020-3786; apib20-14
BUU-2020-04613	Обнаружено	Критический	CVE-2019-1798; apib19-44
BUU-2025-06391	Обнаружено	Критический	VULN-20250116.6; VULN-20250116.52; Chr-2025-6-2; CVE-2025-5068
BUU-2025-00111	Обнаружено	Критический	VULN-20250110.54; Chr-2025-1-7; CVE-2025-0291
BUU-2025-02036	Обнаружено	Критический	VULN-20250216.17; CVE-2025-21407; CVE-2025-21407
BUU-2025-00588	Обнаружено	Критический	VULN-20250117.120; CVE-2025-21176; CVE-2025-21176
BUU-2024-11420	Обнаружено	Критический	Chr-2024-12-18; CVE-2024-12692
BUU-2025-00200	Обнаружено	Критический	VULN-20250117.78; CVE-2025-21241; CVE-2025-21241
BUU-2025-00279	Обнаружено	Критический	VULN-20250117.69; CVE-2025-21243; CVE-2025-21243
BUU-2025-03258	Обнаружено	Критический	VULN-20250311.18; Chr-2025-3-25; CVE-2025-2783
BUU-2025-02126	Обнаружено	Критический	Chr-2024-21612; CVE-2024-26152
BUU-2025-07024	Обнаружено	Критический	VULN-20250253.3; VULN-20250253.12; Chr-2025-6-17; CVE-2025-619
BUU-2025-07733	Обнаружено	Критический	VULN-20250707.15; VULN-20250707.15; Chr-2025-6-30
BUU-2025-00715	Обнаружено	Критический	VULN-20250117.128; VULN-20250127.17; VULN-20250127.37; Chr-2025-1-14
BUU-2025-00752	Обнаружено	Критический	Chr-2025-1-14; CVE-2025-0443
BUU-2025-01218	Обнаружено	Критический	VULN-20200319.10; CVE-2020-3776; apib20-14
BUU-2025-00645	Обнаружено	Критический	VULN-20250117.65; CVE-2025-21409; CVE-2025-21409
BUU-2025-00285	Обнаружено	Критический	VULN-20250117.80; CVE-2025-21223; CVE-2025-21223
BUU-2024-02181	Обнаружено	Критический	CVE-2024-21616; CVE-2024-21616
BUU-2025-00284	Обнаружено	Критический	VULN-20250117.74; CVE-2025-21237; CVE-2025-21237
BUU-2025-00428	Обнаружено	Критический	VULN-20250117.90; CVE-2025-21244; CVE-2025-21244
BUU-2025-06856	Обнаружено	Критический	VULN-20250625.65; CVE-2025-33066; CVE-2025-33066
Проверять по рискам		Группировать по продуктам	
200	423	735	39
2 файла(ов) загружено.			
Всего: 1995			
© ФАУ «ГНИИ ПТЗ ФСБ России»			
Поиск		Помощь	

Выбираю одну критическую уязвимость. В качестве такой уязвимости я беру уязвимость BDU:2025-04706 (CVE-2025-32433)

ScanOVAL				ГЛАВНОЕ	СПРАВКА		
Отображать:		Только обнаруженные					
Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости			
BDU-2025-04862	Обнаружен	Средний	CVE-2025-49686; CVE-2025-49686	Уязвимость повышения привилегий в драйвере Windows TCP/IP (BDU-2025-04862)			
BDU-2025-04861	Обнаружен	Средний	CVE-2025-3141; CVE-2025-53141	Уязвимость несанкционированного получения права Windows Authority Function Driver for WinSock (BDU-2025-04861)			
BDU-2025-04835	Обнаружен	Высокий	VULN-20250326_37; security-bulletin; CVE-2025-0151	Уязвимость в Zoom до 6.3.0, Zoom Client for VDI до 6.2.12, Zoom Room до 6.3.0 (security-bulletin)			
BDU-2025-04706	Критический	Высокий	VULN-20250425_11; VULN-20250512_22; CVE-2025-32433	Уязвимость в Erlang/Otp до 27.3.3, 26.x до 26.2.5.11 и 27.x до 25.3.2.20 (BDU-2025-04706)			
BDU-2025-04668	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3070	Недостаточная проверка неканонических входных данных в расширениях Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)			
BDU-2025-04666	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3071	Неправильная реализация навигации в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)			
BDU-2025-04665	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3072	Неправильная реализация пользовательских вкладок в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)			
BDU-2025-04663	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3073	Неправильная реализация автозаполнения в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)			
BDU-2025-04661	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3074	Неправильная реализация в разделе «Загрузки» в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)			
BDU-2025-04626	Обнаружен	Средний	CVE-2025-27478; CVE-2025-27478	Уязвимость повышения привилегий локального органа безопасности Windows (BDU-2025-04626)			
BDU-2025-04572	Обнаружен	Средний	CVE-2025-0939; python-3922	Уязвимость языка программирования Python до версии 3.9.22 до 3.11.12 (python-3922)			
BDU-2025-04262	Обнаружен	Высокий	CVE-2025-27484; CVE-2025-27484	Уязвимость языка устройства Windows Universal Plug and Play (BDU-2025-04262)			
BDU-2025-04261	Обнаружен	Высокий	VULN-20250416_18; CVE-2025-27487; CVE-2025-27487	Уязвимость удаленного выполнения кода клиента удаленного рабочего стола (BDU-2025-04261)			
BDU-2025-04259	Обнаружен	Критический	CVE-2025-27481; CVE-2025-27481	Уязвимость удаленного выполнения кода службы телефонии Windows (BDU-2025-04259)			
BDU-2025-04254	Обнаружен	Средний	CVE-2025-21204; CVE-2025-21204	Уязвимость повышения привилегий при активации процесса Windows (BDU-2025-04254)			
BDU-2025-04252	Обнаружен	Средний	CVE-2025-20570; CVE-2025-20570	Уязвимость повышения привилегий в Visual Studio Code (BDU-2025-04252)			
BDU-2025-04249	Обнаружен	Средний	CVE-2025-24062; CVE-2025-24062	Уязвимость повышения привилегий в библиотеке Microsoft DWM Core (BDU-2025-04249)			
BDU-2025-04248	Обнаружен	Средний	CVE-2025-24061; CVE-2025-24061	Уязвимость повышения привилегий в библиотеке Microsoft DWM Core (BDU-2025-04248)			
BDU-2025-04247	Обнаружен	Высокий	CVE-2025-29810; CVE-2025-29810	Уязвимость повышения привилегий в доменных службах Active Directory (BDU-2025-04247)			
BDU-2025-04245	Обнаружен	Средний	CVE-2025-27738; CVE-2025-27738	Уязвимость раскрытия информации в файловой системе Windows Resilient File System (BDU-2025-04245)			
BDU-2025-04244	Обнаружен	Средний	CVE-2025-27727; CVE-2025-27727	Уязвимость повышения привилегий установщика Windows (BDU-2025-04244)			
Помощь по поискам		Помощь по продукту		204	253		
Всего: 1359							
<b>Подробности</b>							
Идентификатор уязвимости	<a href="#">BDU-2025-04706</a>						
Результат	Обнаружен						
Уровень опасности уязвимости	Критический						
OVAL							
Название уязвимости	<a href="#">oval:nlu_softwind:win:def:117623</a> (версия 5)						
Описание уязвимости	Уязвимость в Erlang/Otp до 27.3.3, 26.x до 26.2.5.11 и 27.x до 25.3.2.20 (BDU-2025-04706)						
Возможные меры по устранению уязвимости	Версии Erlang/Otp до OTP-27.3.3, OTP-26.2.5.11 и OTP-25.3.2.20 уязвимы к неавтентифицированному удаленному выполнению кода (RCE) через обработку сообщений протокола SSH. Это позволяет выполнять команды без действительных учетных данных. Проблема решена в упомянутых версиях.						
Ссылки на источники	Компенсируем NPKCI <a href="#">VULN-20250425_11</a> NPKCI <a href="#">VULN-20250512_22</a> CVE <a href="#">CVE-2025-32433</a>						
Базовый вектор уязвимости	CVSS: AV:N/AC:Au/N/C:L/C:A/C						
Программное обеспечение	cpe:aerlang-otp:erlang-otp						
Детализация	textfileContent: C:\Program Files\erl10.6\releases\22\OTP_VERSION						
Файл	D:\std_string\learning\labs\защита\каналов\softAllForFSTEC_2025_09_08_create_sign_part2.xml						

Вот описание этой уязвимости на сайте ФСТЭК:

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю  
ФСТЭК России

Государственный научно-исследовательский испытательный институт  
проблем технической защиты информации  
ФАУ «ГНИИ ПТЗИ ФСТЭК России»

Угрозы Уязвимости Тестирование обновлений Документы Обратная связь Обновления Участники Обучение БДУ АСУ ТП ФСТЭК России Помощь Поиск

Главная Список уязвимостей BDU:2025-04706

**ПОСЛЕДНИЕ ИЗМЕНЕНИЯ**

Описание уязвимости	Уязвимость реализации протокола SSH из набора библиотек Erlang/OTP связана с отсутствием проверки подлинности для критически важной функции. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных SSH-пакетов.	Вид
Уязвимое ПО	Вендор  Наименование ПО	Версия ПО  Тип ПО
ООО «Ред Софт»	РЕД ОС (запись в едином реестре российских программ №3751)	7.3 Операционная система
ООО «РусБИТех-Астра»	Astra Linux Special Edition (запись в едином реестре российских программ №369)	1.7 Операционная система
ООО «РусБИТех-Астра»	Astra Linux Special Edition (запись в едином реестре российских программ №369)	1.8 Операционная система
Сообщество свободного программного обеспечения	Erlang/OTP	до 27.3.3 Микропрограммный код
Сообщество свободного программного обеспечения	Erlang/OTP	до 26.2.5.11 Микропрограммный код
Сообщество свободного программного обеспечения	Erlang/OTP	до 25.3.2.20 Микропрограммный код
Cisco Systems Inc.	ConfID	до 7.7.19.1 Сетевое средство Сетевое программное средство
Cisco Systems Inc.	ConfID	до 8.1.16.2 Сетевое средство Сетевое программное

13.09.2025 Уязвимость реализации протокола Address Resolution Protocol (ARP) операционной системы Cisco IOS XR, позволяющая нарушителю вызвать отказ в обслуживании

13.09.2025 Уязвимость интегрионной IoT/SCADA платформы Delta Industrial Automation DiALink, связанная с неверным ограничением имени пути к каталогу с ограниченным доступом, позволяющая нарушителю выполнить произвольный код

12.09.2025 Уязвимость службы Defender Firewall Service операционных систем Windows, позволяющая нарушителю повысить свои привилегии

12.09.2025 Уязвимость класса MapControl операционных систем Windows, позволяющая нарушителю повысить свои привилегии

12.09.2025 Уязвимость программы для просмотра электронных документов в стандарте PDF Foxit PDF Reader (ранее Foxit Reader), связанная с доступом к неинциализированному указателю, позволяющая нарушителю выполнить произвольный код или повредить память

12.09.2025 Уязвимость компонента Broker VM платформы безопасности Cortex XDR, связанная с использованием учетных данных по умолчанию, позволяющая нарушителю получить доступ к внутренним службам на других виртуальных машинах

12.09.2025 Уязвимость обработчика файлов Tet拉格姆 инструмента для статического анализа ядра Checkmarx Prisma Cloud

Вот описание этой уязвимости на cve.org:

**CNA: GitHub (maintainer security advisories)**

Published: 2025-04-16 Updated: 2025-04-16  
Title: Erlang/OTP SSH Vulnerable To Pre-Authentication RCE

**Description**

Erlang/OTP is a set of libraries for the Erlang programming language. Prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, a SSH server may allow an attacker to perform unauthenticated remote code execution (RCE). By exploiting a flaw in SSH protocol message handling, a malicious actor could gain unauthorized access to affected systems and execute arbitrary commands without valid credentials. This issue is patched in versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. A temporary workaround involves disabling the SSH server or to prevent access via firewall rules.

**CWE** 1 Total  
Learn more

- CWE-306: CWE-306: Missing Authentication for Critical Function

**CVSS** 1 Total  
Learn more

Score	Severity	Version	Vector String
10.0	CRITICAL	3.1	CVSS 3.1/AV:N/AC:L/PR:N/U:N/S:C/H/I/H/A:H

**Product Status**  
Learn more

Vendor	Product
erlang	otp

**Versions** 3 Total  
Default Status: unknown

Эта уязвимость имеет следующие параметры:

Оценка: 10.0

Серьезность: Критическая

Вектор: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (версия 3.1)

Тип ошибки: Отсутствие аутентификации для критичной функции (CWE-306)

Описание уязвимости: Уязвимость реализации протокола SSH из набора библиотек Erlang/OTP связана с отсутствием проверки подлинности для критически важной функции. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем отправки специально сформированных SSH-пакетов.

Описание уязвимости на cve.org: Erlang/OTP is a set of libraries for the Erlang programming language. Prior to versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20, a SSH server may allow an attacker to perform unauthenticated remote code execution (RCE). By exploiting a flaw in SSH protocol message handling, a malicious actor could gain unauthorized access to affected systems and execute arbitrary commands without valid credentials. This issue is patched in versions OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. A temporary workaround involves disabling the SSH server or to prevent access via firewall rules.

Возможные меры по устранению уязвимости: Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Устраняю уязвимость.

Проверяю текущую версию Erlang/OTP:

```
C:\Program Files\erl10.6\bin>erl
Eshell V10.6  (abort with ^G)
1> erlang:system_info(version).
"10.6"
2> erlang:system_info(otp_release).
"22"
3>
C:\Program Files\erl10.6\bin>
```

Обновляю Erlang/OTP до последней версии:

ScanOVAL ГЛАВНОЕ СПРАВКА

Отображать: Только обнаруженные

Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2025-04862	Обнаружен	Средний	CVE-2025-49686; CVE-2025-49686	Уязвимость повышения привилегий в драйвере Windows TCP/IP (BDU:2025-04862)
BDU:2025-04861	Обнаружен	Средний	CVE-2025-53141; CVE-2025-53141	Уязвимость несанкционированного получения прав Windows Ancillary Function Driver for WinSock (BDU:2025-04861)
BDU:2025-04835	Обнаружен	Высокий	VULN-20250326-37; security-bulletin; CVE-2025-0151	Уязвимость в Zoom до 6.3.0, Zoom Client for VDI до 6.2.12, Zoom Rooms до 6.3.0 (security-bulletin)
BDU:2025-04706	Обнаружен	Критический	VULN-20250425-11; VULN-20250512-22; CVE-2025-32433	Уязвимость в Erlang/OTP до 27.3.3, 26.x до 26.2.5.11 и 27.x до 25.3.2.20 (BDU:2025-04706)
BDU:2025-04668	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3070	Недостаточная проверка ненадежных входных данных в расширении Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04666	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3071	Неправильная реализация навигации в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04665	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3072	Неправильная реализация пользовательских вкладок в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04663	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3073	Неправильная реализация пользовательских вкладок в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04661	Обнаружен	Средний	Chr-2025-4-1; CVE-2025-3074	Неправильная реализация пользовательских вкладок в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04626	Обнаружен	Средний	CVE-2025-27476; CVE-202	Erlang OTP 28 Setup
BDU:2025-04572	Обнаружен	Средний	CVE-2025-0938; python-3	Choose Components
BDU:2025-04262	Обнаружен	Высокий	CVE-2025-27484; CVE-202	Choose which features of Erlang OTP 28 you want to install.
BDU:2025-04261	Обнаружен	Высокий	VULN-20250416-18; CVE-2	Check the components you want to install and uncheck the components you don't want to
BDU:2025-04259	Обнаружен	Критический	CVE-2025-27481; CVE-202	install. Click Next to continue.
BDU:2025-04254	Обнаружен	Средний	CVE-2025-21204; CVE-202	Select components to install:
BDU:2025-04252	Обнаружен	Средний	CVE-2025-20570; CVE-202	Position your mouse over a component to see its description.
BDU:2025-04249	Обнаружен	Средний	CVE-2025-24062; CVE-202	Microsoft DLL's (present)
BDU:2025-04248	Обнаружен	Средний	CVE-2025-24060; CVE-202	Erlang
BDU:2025-04247	Обнаружен	Высокий	CVE-2025-29810; CVE-202	Development
BDU:2025-04245	Обнаружен	Средний	CVE-2025-27738; CVE-202	Associations
BDU:2025-04244	Обнаружен	Средний	CVE-2025-27727; CVE-202	Erlang Documentation

Были применены на рисках: 200 из 433 из 39

Было загружено: 2 файла(ов)

Всего: 1395

Подробности

Идентификатор уязвимости: BDU:2025-04706

Результат: Обнаружен

Уровень опасности уязвимости OVAL: Критический

Название уязвимости: [vulnerability\\_softwin.def117623](#) (версия 5)

Описание уязвимости: Уязвимость в Erlang/OTP до 27.3.3, 26.x до 26.2.5.11 и 27.x до 25.3.2.20 (BDU:2025-04706)

Возможные меры по устранению уязвимости: Версии Erlang/OTP до OTP-27.3.3, OTP-26.2.5.11 и OTP-25.3.2.20 уязвимы к неавтентифицированному удаленному выполнению кода (RCE) через обработку сообщений протокола SSH. Это позволяет выполнять команды без действительных учетных данных. Проблема решена в упомянутых версиях. Временное решение — отключить SSH-сервер или ограничить доступ с помощью правил брандмауэра.

Ссылки на источники: Компенсирует: NCKI [VULN-20250425.11](#), NCKI [VULN-20250512.22](#), CVE [CVE-2025-32433](#)

Базовый вектор уязвимости: CVSS: 3.0/AV:N/AC:L/Au:N/C:L/I:C/A:C

Программное обеспечение: cpe:/erlang:otp:erlang-otp

Детализация: textfile:content: C:\Program Files\erl10.6\releases\22\OTP.VERSIO

Файл: D:\std\_string\learning\labs\защита\_каналов\softAllForFSTEC\_2025\_09\_08\_create\_sign\_part2.xml

Проверяю версию Erlang/OTP после обновления:

(C:\Program Files\Erlang OTP\bin) - Far 3.0.5511 v64

```
C:\Program Files\Erlang OTP\bin>erl
Erlang/OTP 28 [erts-16.0.3] [source] [64-bit] [smp:16:16] [ds:16:16:10] [async-threads:1] [jit:ns]

Eshell V16.0.3 (press Ctrl+G to abort, type help(). for help)
1> erlang:system_info(version).
"16.0.3"
2> erlang:system_info(otp_release).
"28"
3>
BREAK: (a)abort (A)abort with dump (c)continue (p)roc info (i)info
      (l)oaded (v)ersion (k)ill (D)b-tables (d)istribution
a

C:\Program Files\Erlang OTP\bin>
```

1Help 2UserMn 3View 4Edit 5Copy 6RenMov 7WkFold 8Delete 9ConfMn 10Quit 11Plugin 12Screen

Запускаю сканирование хостовой машины с помощью ScanOVAL после устранения уязвимости:

ScanOVAL				
ГЛАВНОЕ СПРАВКА				
Отобразить: Все уязвимости				
Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости
BDU:2025-09563		Низкий	CVE-2024-10228	Уязвимость в Vagrant VMware Utility до 1.0.23 (BDU:2025-09563)
BDU:2025-09499		Высокий	CVE-2025-49125; security-9#Fixed_in_Apache_Tomcat_9.0.105; secur	Уязвимость в Apache Tomcat с 11.0.0-M1 до 11.0.7 и < 10.1.0-M1 до 10.1.41 и < 9.0.0-M1 до 9.0.105 (security-9#Fixed_in_Apache_Tomcat_9.0.105; security-10#Fixed_in_Apache_Tomcat_10.1.41,...)
BDU:2025-09498		Высокий	CVE-2025-46701; security-9#Fixed_in_Apache_Tomcat_9.0.105; secur	Уязвимость обхода ограничения безопасности CGI в Apache Tomcat с 11.0.0-M1 до 11.0.7 и < 10.1.0-M1 до 10.1.41 и < 9.0.0-M1 до 9.0.105 (security-9#Fixed_in_Apache_Tomcat_9.0.105; security-10#Fixed_in_Apache_Tomcat_10.1.41,...)
BDU:2025-09493		Средний	CVE-2025-54090; vulnerabilities_24#CVE-2025-54090	Уязвимость в Apache HTTP Server версии 2.4.44 (vulnerabilities_24#CVE-2025-54090)
BDU:2025-09488		Высокий	CVE-2025-54090; vulnerabilities_24#CVE-2025-54090	Уязвимость в Apache HTTP Server версии 2.4.44 (vulnerabilities_24#CVE-2025-54090)
BDU:2025-09477		Высокий	CVE-2025-54135	Уязвимость в Cursor до 1.3.9 (BDU:2025-09488)
BDU:2025-09475		Высокий	CVE-2025-53786; CVE-2025-53786	Уязвимость доступа к освобожденной памяти в Google Chrome до 139.0.7258.66 (Chr-2025-8-5)
BDU:2025-09474		Средний	Chr-2025-8-5; CVE-2025-8580	Ошибка реализации в Google Chrome до 139.0.7258.66 (Chr-2025-8-5)
BDU:2025-09475		Средний	CVE-2025-8580; CVE-2025-8580	Ошибка реализации в Microsoft Edge (BDU:2025-09475)
BDU:2025-09470		Средний	CVE-2024-52905; 7232336	Уязвимость в IBM DB2 до 12.1.0.986 (7232336)
BDU:2025-09463		Высокий	Chr-2025-8-5; CVE-2025-8578	Уязвимость доступа к освобожденной памяти в Google Chrome до 139.0.7258.66 (Chr-2025-8-5)
BDU:2025-09463		Высокий	CVE-2025-8578; CVE-2025-8578	Уязвимость доступа к освобожденной памяти в Microsoft Exchange Server Hybrid Deployment (BDU:2025-09477)
BDU:2025-09462		Критический	VUUN-20250730-11; CVE-2025-8040; mfsa2025-56; mfsa2025-59; mfsa	Уязвимость в Thunderbird до 140.1 и 141.0, Firefox ESR до 140.1, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-63)
BDU:2025-09461		Высокий	VUUN-20250730-9; CVE-2025-8039; mfsa2025-56; mfsa2025-59; mfsa	Уязвимость в Thunderbird до 140.1 и 141.0, Firefox ESR до 140.1, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-63)
BDU:2025-09460		Высокий	VUUN-20250730-4; CVE-2025-8036; mfsa2025-56; mfsa2025-59; mfsa	Уязвимость в Thunderbird до 140.1 и 141.0, Firefox ESR до 140.1, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-63)
BDU:2025-09459		Критический	VUUN-20250730-10; CVE-2025-8034; mfsa2025-56; mfsa2025-57; mfsa	Уязвимость в Thunderbird начиная с 140.0 до 140.1 и до 128.13, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-62,...)
BDU:2025-09458		Критический	VUUN-20250730-10; CVE-2025-8034; mfsa2025-56; mfsa2025-57; mfsa	Уязвимость в Thunderbird начиная с 140.0 до 140.1 и до 128.13 и до 115.26, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-62,...)
BDU:2025-09457		Высокий	VUUN-20250730-3; CVE-2025-8029; mfsa2025-56; mfsa2025-58; mfsa	Уязвимость в Thunderbird начиная с 140.0 до 140.1 и до 128.13 и 141.0, Firefox ESR начиная с 140.0 до 140.1 и начиная с 128.0 до 128.13 и до 115.26, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-62,...)
BDU:2025-09456		Средний	CVE-2025-8581; CVE-2025-8581	Выполнение "AllForFSTEC_2025_09_08_create_sign_part1.xml" (1/2) ...
BDU:2025-09456		Средний	Chr-2025-8-5; CVE-2025-8581	Ошибка реализации в Google Chrome до 139.0.7258.66 (Chr-2025-8-5)
BDU:2025-09455		Средний	CVE-2025-8583; CVE-2025-8583	Недостаточная проверка ненадежных входных данных в Microsoft Edge (BDU:2025-09454)
BDU:2025-09455		Средний	Chr-2025-8-5; CVE-2025-8583	Недостаточная проверка ненадежных входных данных в Google Chrome до 139.0.7258.66 (Chr-2025-8-5)
BDU:2025-09454		Средний	CVE-2025-8582; CVE-2025-8582	Уязвимость в Thunderbird до 140.1 и 141.0, Firefox ESR до 140.1, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-63)
BDU:2025-09454		Средний	Chr-2025-8-5; CVE-2025-8582	Уязвимость в Thunderbird начиная с 140.0 до 140.1 и до 128.13 и 141.0, Firefox ESR начиная с 140.0 до 140.1 и начиная с 128.0 до 128.13 и до 115.26, Firefox до 141.0 (mfsa2025-56, mfsa2025-59, mfsa2025-61, mfsa2025-62,...)
BDU:2025-09448		Высокий	CVE-2025-8416	Уязвимость в Cisogel до 1.3 (BDU:2025-09448)
BDU:2025-09447		Высокий	CVE-2025-83286; 5670	Уязвимость в Графическом драйвере NVIDIA R535, R570, и R575 (5670)
BDU:2025-09445		Средний	CVE-2025-8376; 5670	Уязвимость в Графическом драйвере NVIDIA R535, R570, и R575 (5670)
BDU:2025-09444		Высокий	VUUN-20250821-66; CVE-2025-7025	Уязвимость в Rockwell Automation Arena до 16.20.10 (BDU:2025-09444)
BDU:2025-09421		Критический	Chr-2025-7-29; CVE-2025-8292	Уязвимость доступа к освобожденной памяти в Google Chrome до 138.0.7204.183 (Chr-2025-7-29)
BDU:2025-09421		Критический	CVE-2025-8292; CVE-2025-8292	Уязвимость доступа к освобожденной памяти в Microsoft Edge (BDU:2025-09421)
BDU:2025-09419		Критический	VUUN-20250730-24; CVE-2025-8010	Уязвимость, связанная с подменой типа в Microsoft Edge (BDU:2025-09419)
BDU:2025-09419		Критический	VUUN-20250730-24; CVE-2025-7-22; CVE-2025-8010	Уязвимость, связанная с подменой типа в Google Chrome до 138.0.7204.168 (Chr-2025-7-22)
BDU:2025-09418		Критический	VUUN-20250730-23; CVE-2025-7-22; CVE-2025-8011	Уязвимость, связанная с подменой типа в Google Chrome до 138.0.7204.168 (Chr-2025-7-22)
BDU:2025-09412		Средний	CVE-2025-23286; 5670	Уязвимость, связанная с подменой типа в Microsoft Edge (BDU:2025-09412)
BDU:2025-09411		Низкий	CVE-2025-23287; 5670	Уязвимость в Графическом драйвере NVIDIA R535, R570, и R575 (5670)

Всего: 32252

Подробности				
© ФАУ «ГИИИ ПТЗИ ФСТЭК России»				

Видно, что уязвимости BDU:2025-04706 (CVE-2025-32433) среди найденных уязвимостей больше нет

ScanOVAL				
ГЛАВНОЕ СПРАВКА				
Отобразить: Только обнаруженные				
Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости
BDU:2025-05405		Обнаружена	CVE-2025-2407; 3072	Уязвимость в PostgreSQL с 17.0 до 17.5 и < 16.0 до 16.9 и < 15.0 до 15.13 и < 14.0 до 14.18 и < 13.0 до 13.21 (3072)
BDU:2025-05209		Обнаружена	CVE-2025-0167; CVE-2025-0167	Уязвимость в cURL/libcurl с 7.76.0 до 8.11.1 (BDU:2025-05209)
BDU:2025-04983		Обнаружена	CVE-2025-26675; CVE-2025-26675	Подсистема Windows для уязвимости Linux, приводящая к повышению привилегий (BDU:2025-04983)
BDU:2025-04982		Средний	CVE-2025-27467; CVE-2025-27467	Уязвимость Windows Digital Media, приводящая к повышению привилегий (BDU:2025-04982)
BDU:2025-04979		Обнаружена	CVE-2025-26640; CVE-2025-26648	Уязвимость ядра Windows, приводящая к повышению привилегий (BDU:2025-04979)
BDU:2025-04977		Обнаружена	CVE-2025-36679; CVE-2025-26679	Уязвимость повышения привилегий службы RPC Endpoint Mapper (BDU:2025-04977)
BDU:2025-04976		Обнаружена	CVE-2025-27731; CVE-2025-27731	Уязвимость повышения привилегий службы RPC Endpoint Mapper (BDU:2025-04976)
BDU:2025-04975		Средний	CVE-2025-27731; CVE-2025-27737	Уязвимость повышения привилегий службы RPC Endpoint Mapper (BDU:2025-04975)
BDU:2025-04975		Средний	CVE-2025-27737; CVE-2025-27737	Уязвимость повышения привилегий службы RPC Endpoint Mapper (BDU:2025-04975)
BDU:2025-04921		Критический	VUUN-20250425-9; VUUN-20250420-5; Chr-2025-4-15; CVE-2025-3620	Использование после обновления в USB в Google Chrome до 135.0.7049.95 (Chr-2025-4-15)
BDU:2025-04862		Средний	CVE-2025-49866; CVE-2025-49866	Уязвимость повышения привилегий в драйвере Windows TCP/IP (BDU:2025-04862)
BDU:2025-04861		Средний	CVE-2025-3141; CVE-2025-53141	Уязвимость несанкционированного получения прав Windows Ancillary Function Driver for WinSock (BDU:2025-04861)
BDU:2025-04835		Обнаружена	VUUN-20250426-37; security-bulletin; CVE-2025-0151	Уязвимость в Zoom для VDI до 6.2.12, Zoom Rooms до 6.3.0 (security-bulletin)
BDU:2025-04668		Обнаружена	Chr-2025-4-1; CVE-2025-3070	Недостаточная проверка ненадежных входных данных в расширении Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04668		Средний	Chr-2025-4-1; CVE-2025-3070	Неправильная реализация навигации в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04666		Обнаружена	Chr-2025-4-1; CVE-2025-3071	Неправильная реализация пользовательских вкладок в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04665		Средний	Chr-2025-4-1; CVE-2025-3072	Неправильная реализация автозаполнения в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04663		Средний	Chr-2025-4-1; CVE-2025-3073	Неправильная реализация в разделе «загрузки» в Google Chrome до версии 135.0.7049.52 (Chr-2025-4-1)
BDU:2025-04661		Средний	Chr-2025-3074; CVE-2025-27478	Уязвимость повышения привилегий в драйвере Windows TCP/IP (BDU:2025-04626)
BDU:2025-04572		Средний	CVE-2025-9398; python-3922	Уязвимость в Python с версии 3.9.22 до 3.11.12 (python-3922)
BDU:2025-04262		Обнаружена	CVE-2025-27484; CVE-2025-27484	Уязвимость ядра устройства Windows Universal Plug and Play (BDU:2025-04262)
BDU:2025-04261		Высокий	VUUN-20250416-18; CVE-2025-27487; CVE-2025-27487	Уязвимость удаленного выполнения кода клиента удаленного рабочего стола (BDU:2025-04261)
BDU:2025-04259		Критический	CVE-2025-27481; CVE-2025-27481	Уязвимость удаленного выполнения кода службы телефонии Windows (BDU:2025-04259)
BDU:2025-04254		Обнаружена	CVE-2025-21204; CVE-2025-21204	Уязвимость повышения привилегий при активации процесса Windows (BDU:2025-04254)
BDU:2025-04252		Средний	CVE-2025-20570; CVE-2025-20570	Уязвимость повышения привилегий в Visual Studio Code (BDU:2025-04252)
BDU:2025-04249		Средний	CVE-2025-24062; CVE-2025-24062	Уязвимость повышения привилегий в библиотеке Microsoft DWM Core (BDU:2025-04249)
BDU:2025-04248		Средний	CVE-2025-24060; CVE-2025-24060	Уязвимость повышения привилегий в библиотеке Microsoft DWM Core (BDU:2025-04248)
BDU:2025-04247		Обнаружена	CVE-2025-29810; CVE-2025-29810	Уязвимость повышения привилегий в доменных службах Active Directory (BDU:2025-04247)
BDU:2025-04245		Обнаружена	CVE-2025-27738; CVE-2025-27738	Уязвимость разрыва информации в файловой системе Windows Resilient File System (BDU:2025-04245)
BDU:2025-04243		Средний	CVE-2025-27730; CVE-2025-27730	Уязвимость повышения привилегий установщика Windows (BDU:2025-04244)
BDU:2025-04241		Средний	CVE-2025-26669; CVE-2025-26669	Уязвимость разрыва информации службы маршрутизации и удаленного доступа Windows (BDU:2025-04241)
BDU:2025-04240		Средний	CVE-2025-26681; CVE-2025-26681	Уязвимость Win32, приводящая к повышению привилегий (BDU:2025-04240)
BDU:2025-04238		Обнаружена	CVE-2025-27490; CVE-2025-27490	Уязвимость повышения привилегий службы Bluetooth в Windows (BDU:2025-04238)
BDU:2025-04233		Средний	CVE-2025-24074; CVE-2025-24074	Уязвимость повышения привилегий в библиотеке Microsoft DWM Core (BDU:2025-04233)
BDU:2025-04227		Обнаружена	CVE-2025-24058; CVE-2025-24058	Уязвимость повышения привилегий в библиотеке Windows DWM Core (BDU:2025-04227)
BDU:2025-04217		Обнаружена	CVE-2025-21222; CVE-2025-21222	Уязвимость удаленного выполнения кода службы телефонии Windows (BDU:2025-04217)

Уязвимость

Подробности				
© ФАУ «ГИИИ ПТЗИ ФСТЭК России»				

Всего: 1391