Отчет Vulners PDF

Название программы: LibreOffice

Версия программы: 6.0.7

Список CVE (Всего 18):

- LibreOffice 6.0.7 / 6.1.3 - Macro Code Execution Exploit
- LibreOffice < 6.2.6 Macro - Python Code Execution Exploit
- LibreOffice Security Advisory
- CVE-2019-9847
- CVE-2019-9848
- CVE-2019-9849
- CVE-2019-9850
- CVE-2019-9851
- CVE-2019-9852
- CVE-2020-12802
- CVE-2020-12803
- LibreOffice < 6.0.7 / 6.1.3 - Macro Code Execution (Metasploit)
- LibreOffice < 6.2.6 Macro - Python Code Execution (Metasploit)
- LibreOffice 6.2.6 Macro - Python Code Execution (Metasploit)
- LibreOffice Macro Python Code Execution
- LibreOffice Macro Code Execution
- LibreOffice Macro Code Execution
- LibreOffice Macro Python Code Execution

Название программы: 7-Zip

Версия программы: 18.03

Список CVE (Всего 1):

- CVE-2018-10115

Название программы: Adobe Reader

Версия программы: 18.009.20050

Список CVE (Всего 168):

- CVE-2018-12754
- CVE-2018-12755
- CVE-2018-12756
- CVE-2018-12757
- CVE-2018-12758
- CVE-2018-12760
- CVE-2018-12761
- CVE-2018-12762
- CVE-2018-12763
- CVE-2018-12764
- CVE-2018-12765
- CVE-2018-12766
- CVE-2018-12767
- CVE-2018-12768
- CVE-2018-12770
- CVE-2018-12771
- CVE-2018-12772
- CVE-2018-12773
- CVE-2018-12774
- CVE-2018-12776
- CVE-2018-12777
- CVE-2018-12779
- CVE-2018-12780
- CVE-2018-12781
- CVE-2018-12782
- CVE-2018-12783
- CVE-2018-12784
- CVE-2018-12785
- CVE-2018-12786
- CVE-2018-12787
- CVE-2018-12788
- CVE-2018-12789
- CVE-2018-12790
- CVE-2018-12791
- CVE-2018-12792
- CVE-2018-12793
- CVE-2018-12794
- CVE-2018-12795
- CVE-2018-12796
- CVE-2018-12797
- CVE-2018-12798
- CVE-2018-12799
- CVE-2018-12802
- CVE-2018-12803
- CVE-2018-12808
- CVE-2018-12812
- CVE-2018-12815
- CVE-2018-4917
- CVE-2018-4918

- CVE-2018-4947
- CVE-2018-4948
- CVE-2018-4949
- CVE-2018-4950
- CVE-2018-4951
- CVE-2018-4952
- CVE-2018-4953
- CVE-2018-4954
- CVE-2018-4955
- CVE-2018-4956
- CVE-2018-4957
- CVE-2018-4958
- CVE-2018-4959
- CVE-2018-4960
- CVE-2018-4961
- CVE-2018-4962
- CVE-2018-4963
- CVE-2018-4964
- CVE-2018-4965
- CVE-2018-4966
- CVE-2018-4967
- CVE-2018-4968
- CVE-2018-4969
- CVE-2018-4970
- CVE-2018-4971
- CVE-2018-4972
- CVE-2018-4973
- CVE-2018-4974
- CVE-2018-4975
- CVE-2018-4976
- CVE-2018-4977
- CVE-2018-4978
- CVE-2018-4979
- CVE-2018-4980
- CVE-2018-4981
- CVE-2018-4982
- CVE-2018-4983
- CVE-2018-4984
- CVE-2018-4985
- CVE-2018-4986
- CVE-2018-4987
- CVE-2018-4988
- CVE-2018-4989
- CVE-2018-4990
- CVE-2018-4993
- CVE-2018-4995
- CVE-2018-4996
- CVE-2018-4997
- CVE-2018-4998
- CVE-2018-4999
- CVE-2018-5009
- CVE-2018-5010
- CVE-2018-5011
- CVE-2018-5012
- CVE-2018-5014
- CVE-2018-5015
- CVE-2018-5016
- CVE-2018-5017
- CVE-2018-5018
- CVE-2018-5019
- CVE-2018-5020
- CVE-2018-5021
- CVE-2018-5022
- CVE-2018-5023
- CVE-2018-5024
- CVE-2018-5025
- CVE-2018-5026
- CVE-2018-5027
- CVE-2018-5028
- CVE-2018-5029
- CVE-2018-5030
- CVE-2018-5031
- CVE-2018-5032
- CVE-2018-5033
- CVE-2018-5034
- CVE-2018-5035
- CVE-2018-5036
- CVE-2018-5037
- CVE-2018-5038
- CVE-2018-5039
- CVE-2018-5040
- CVE-2018-5041
- CVE-2018-5042
- CVE-2018-5043
- CVE-2018-5044

- CVE-2018-5045
- CVE-2018-5046
- CVE-2018-5047
- CVE-2018-5048
- CVE-2018-5049
- CVE-2018-5050
- CVE-2018-5051
- CVE-2018-5052
- CVE-2018-5053
- CVE-2018-5054
- CVE-2018-5055
- CVE-2018-5056
- CVE-2018-5057
- CVE-2018-5058
- CVE-2018-5059
- CVE-2018-5060
- CVE-2018-5061
- CVE-2018-5062
- CVE-2018-5063
- CVE-2018-5064
- CVE-2018-5065
- CVE-2018-5066
- CVE-2018-5067
- CVE-2018-5068
- CVE-2018-5069
- CVE-2018-5070
- BADPDF Malicious PDF Creator
- BADPDF Malicious PDF Creator
- SRC-2018-0021 : Adobe Acrobat Pro DC HTML2PDF HTML Parsing img setAttribute Use-After-Free Remote Code Execution Vulnerability
- SRC-2018-0022 : Adobe Acrobat Pro DC HTML2PDF HTML Parsing window.getMatchedCSSRules Use-After-Free Remote Code Execution Vulnerability
- SRC-2018-0023 : Adobe Acrobat Pro DC XPS OpenType Font Parsing idDelta Heap Buffer Overflow Remote Code Execution Vulnerability
- Adobe Acrobat Reader DC Net.Discovery.queryServices Remote Code Execution Vulnerability(CVE-2018-4996)
- Adobe Acrobat Reader DC ANFancyAlertImpl Remote Code Execution Vulnerability(CVE-2018-4947)
- Microsoft Windows Kernel 'Win32k.sys' Local Privilege Escalation Vulnerability(CVE-2018-8120)

Название программы: nginx

Версия программы: 1.14.0

Список CVE (Всего 19):

- Exploit for Off-by-one Error in F5 Nginx
- NGINX -- 1-byte memory overwrite in resolver
- nginx 1.20.0 DNS Resolver Off-By-One Heap Write Exploit
- Nginx 1.20.0 - Denial of Service Exploit
- Exploit for Off-by-one Error in F5 Nginx
- Exploit for Off-by-one Error in F5 Nginx
- nginx -- Two vulnerabilities
- NGINX -- Multiple vulnerabilities
- NGINX -- Multiple vulnerabilities
- Exploit for Uncontrolled Resource Consumption in F5 Nginx
- nginx-devel -- SSL session reuse vulnerability
- Exploit for Off-by-one Error in F5 Nginx
- nginx -- Vulnerability in the ngx_http_mp4_module
- Exploit for Off-by-one Error in F5 Nginx
- NGINX -- HTTP request smuggling
- Exploit for Out-of-bounds Write in F5 Nginx
- Nginx 1.20.0 - Denial of Service (DOS)
- nginx 1.20.0 DNS Resolver Off-By-One Heap Write
- Nginx 1.20.0 Denial Of Service

Название программы: Apache HTTP Server

Версия программы: 2.4.29

Список CVE (Всего 110):

- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for CVE-2024-38475
- Apache 2.4.17 < 2.4.38 - apache2ctl graceful (logrotate) Local Privilege Escalation Exploit
- Apache Httpd mod_proxy - Error Page Cross-Site Scripting Vulnerability
- Apache Httpd mod_rewrite - Open Redirects Vulnerability
- Apache 2 HTTP2 Module Concurrent Pool Usage Vulnerability
- Apache 2.4.x - Buffer Overflow Exploit
- Apache 2.4.55 mod_proxy HTTP Request Smuggling Exploit
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for CVE-2014-4210
- Exploit for CVE-2024-38475
- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for HTTP Request Smuggling in Apache Http Server
- Exploit for Cross-site Scripting in Apache Http Server
- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for Allocation of Resources Without Limits or Throttling in Apache Http Server
- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for Exposure of Resource to Wrong Sphere in Apache Http Server
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for HTTP Request Smuggling in Apache Http Server
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Server-Side Request Forgery in Apache Http Server

- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for CVE-2014-4210
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for HTTP Request Smuggling in Apache Http Server
- Exploit for CVE-2023-38709
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Out-of-bounds Write in Apache Http Server
- Exploit for Allocation of Resources Without Limits or Throttling in Apache Http Server
- Exploit for Exposure of Resource to Wrong Sphere in Apache Http Server
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- CVE-2006-20001
- CVE-2017-15710
- CVE-2017-15715
- CVE-2018-11763
- CVE-2018-1283
- CVE-2018-1301
- CVE-2018-1302
- CVE-2018-1303
- CVE-2018-1312
- CVE-2018-1333
- CVE-2018-17189
- CVE-2018-17199
- CVE-2019-0196
- CVE-2019-0211
- CVE-2019-0217
- CVE-2019-0220
- CVE-2019-10081
- CVE-2019-10082
- CVE-2019-10092
- CVE-2019-10098
- CVE-2019-17567
- CVE-2019-9517
- CVE-2020-11993
- CVE-2020-13938
- CVE-2020-1927
- CVE-2020-1934
- CVE-2020-35452
- CVE-2020-9490
- CVE-2021-26690
- CVE-2021-26691
- CVE-2021-33193
- CVE-2021-34798
- CVE-2021-39275
- CVE-2021-40438
- CVE-2021-44224
- CVE-2021-44790
- CVE-2022-22719
- CVE-2022-22720
- CVE-2022-22721
- CVE-2022-23943
- CVE-2022-26377
- CVE-2022-28330
- CVE-2022-28614
- CVE-2022-28615
- CVE-2022-29404
- CVE-2022-30556
- CVE-2022-31813
- CVE-2022-36760
- CVE-2022-37436
- CVE-2023-25690
- CVE-2023-31122
- CVE-2023-38709
- CVE-2023-45802
- CVE-2024-27316
- CVE-2024-38474
- CVE-2024-38475
- CVE-2024-38476
- CVE-2024-38477
- CVE-2024-39573
- CVE-2024-40898
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Server-Side Request Forgery in Apache Http Server
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Exposure of Resource to Wrong Sphere in Apache Http Server
- Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation
- Apache 2.4.x - Buffer Overflow
- Apache 2.4.17 2.4.38 - apache2ctl graceful logrotate Local Privilege Escalation
- Exploit for HTTP Request Smuggling in Apache Http Server
- Exploit for Uncontrolled Resource Consumption in Ietf Http
- Exploit for Server-Side Request Forgery in Apache Http Server

- CARPE (DIEM) Apache 2.4.x Local Privilege Escalation
- Apache 2.4.x Buffer Overflow
- Apache 2.4.55 mod_proxy HTTP Request Smuggling

Название программы: DjVu Reader

Версия программы: 2.0.0.27

Уязвимостей не обнаружено.

Название программы: Wireshark

Версия программы: 2.6.1

Список CVE (Всего 50):

- CVE-2018-14339
- CVE-2018-14340
- CVE-2018-14341
- CVE-2018-14342
- CVE-2018-14343
- CVE-2018-14344
- CVE-2018-14367
- CVE-2018-14368
- CVE-2018-14369
- CVE-2018-14370
- CVE-2018-14438
- CVE-2018-16056
- CVE-2018-16057
- CVE-2018-16058
- CVE-2018-18225
- CVE-2018-18226
- CVE-2018-18227
- CVE-2018-19622
- CVE-2018-19623
- CVE-2018-19624
- CVE-2018-19625
- CVE-2018-19626
- CVE-2018-19627
- CVE-2018-19628
- CVE-2019-10894
- CVE-2019-10895
- CVE-2019-10896
- CVE-2019-10899
- CVE-2019-10901
- CVE-2019-10903
- CVE-2019-12295
- CVE-2019-13619
- CVE-2019-16319
- CVE-2019-19553
- CVE-2019-5716
- CVE-2019-5717
- CVE-2019-5718
- CVE-2019-5719
- CVE-2019-9208
- CVE-2019-9209
- CVE-2019-9214
- CVE-2020-11647
- CVE-2020-13164
- CVE-2020-25862
- CVE-2020-25863
- CVE-2020-26575
- CVE-2020-9428
- CVE-2020-9430
- CVE-2020-9431
- CVE-2023-2906

Название программы: Notepad++

Версия программы: 8.0

Список CVE (Всего 1):

- CVE-2023-6401

Название программы: Mozilla Firefox

Версия программы: 61.0.1

Список CVE (Всего 1146):

- firefox -- multiple vulnerabilities
- Exploit for CVE-2024-4367
- mozilla -- multiple vulnerabilities
- mozilla -- multiple vulnerabilities
- mozilla -- multiple vulnerabilities
- Exploit for Improper Authentication in Microsoft
- mozilla -- multiple vulnerabilities
- firefox -- multiple vulnerabilities
- Mozilla -- Stored passwords in 'Saved Logins' can be copied without master password entry
- Exploit for CVE-2023-40477
- mozilla -- multiple vulnerabilities

- Firefox 66.0.1 - Array.prototype.slice Buffer Overflow Exploit
- Spidermonkey - IonMonkey Type Inference is Incorrect for Constructors Entered via OSR
- SpiderMonkey - IonMonkey Compiled Code Fails to Update Inferred Property Types (Type Confusion)
- Spidermonkey IonMonkey JS_OPTIMIZED_OUT Value Leak Exploit
- Spidermonkey - IonMonkey Unexpected ObjectGroup in ObjectGroupDispatch Operation Exploit
- Mozilla Spidermonkey - IonMonkey (Array.prototype.pop) Type Confusion Exploit
- Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack Exploit
- Mozilla Firefox 72 IonMonkey - JIT Type Confusion Exploit
- Mozilla Firefox 67 - Array.pop JIT Type Confusion Exploit
- Firefox MCallGetProperty Write Side Effects Use-After-Free Exploit
- Exploit for Type Confusion in Mozilla Firefox
- Exploit for CVE-2024-4367
- mozilla -- multiple vulnerabilities
- Exploit for CVE-2024-4367
- Exploit for CVE-2014-4210
- firefox -- use-after-free code execution
- firefox -- Crash in TransportSecurityInfo due to cached data
- Exploit for Prototype Pollution in Mozilla Firefox
- Exploit for Out-of-bounds Write in Webmproject Libvpx
- Mozilla -- multiple vulnerabilities
- mozilla -- code execution via Quicktime media-link files
- mozilla -- multiple vulnerabilities
- Exploit for CVE-2022-44666
- Exploit for Use After Free in Mozilla Firefox
- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for CVE-2024-4367
- Exploit for Type Confusion in Mozilla Firefox
- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for Vulnerability in Google Chrome
- firefox -- multiple vulnerabilities
- firefox -- multiple vulnerabilities
- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for Out-of-bounds Write in Webmproject Libvpx
- Exploit for Incorrect Authorization in Apple Macos
- firefox -- Potential memory corruption and exploitable crash
- mozilla -- multiple vulnerabilities
- firefox -- Multiple vulnerabilities
- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for Improper Authentication in Microsoft
- Exploit for Out-of-bounds Write in Webmproject Libvpx
- Exploit for CVE-2014-4210
- firefox -- multiple vulnerabilities
- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for CVE-2024-4367
- mozilla firefox -- protocol information guessing
- Exploit for Use After Free in Mozilla Firefox
- mozilla -- multiple vulnerabilities
- Exploit for CVE-2024-4367
- Exploit for Type Confusion in Mozilla Thunderbird
- Exploit for Type Confusion in Mozilla Thunderbird
- mozilla -- multiple vulnerabilities
- mozilla -- multiple vulnerabilities
- Exploit for CVE-2024-4367
- CVE-2018-12375
- CVE-2018-12376
- CVE-2018-12377
- CVE-2018-12378
- CVE-2018-12379
- CVE-2018-12381
- CVE-2018-12382
- CVE-2018-12383
- CVE-2018-12385
- CVE-2018-12386
- CVE-2018-12387
- CVE-2018-12388
- CVE-2018-12390
- CVE-2018-12391
- CVE-2018-12392
- CVE-2018-12393
- CVE-2018-12395
- CVE-2018-12396
- CVE-2018-12397
- CVE-2018-12398
- CVE-2018-12399
- CVE-2018-12400
- CVE-2018-12401
- CVE-2018-12402
- CVE-2018-12403
- CVE-2018-12405
- CVE-2018-12406
- CVE-2018-12407
- CVE-2018-18492
- CVE-2018-18493
- CVE-2018-18494
- CVE-2018-18495

- CVE-2018-18496
- CVE-2018-18497
- CVE-2018-18498
- CVE-2018-18499
- CVE-2018-18500
- CVE-2018-18501
- CVE-2018-18502
- CVE-2018-18503
- CVE-2018-18504
- CVE-2018-18505
- CVE-2018-18506
- CVE-2018-18510
- CVE-2018-18511
- CVE-2019-11691
- CVE-2019-11692
- CVE-2019-11693
- CVE-2019-11694
- CVE-2019-11695
- CVE-2019-11696
- CVE-2019-11697
- CVE-2019-11698
- CVE-2019-11699
- CVE-2019-11700
- CVE-2019-11701
- CVE-2019-11702
- CVE-2019-11707
- CVE-2019-11708
- CVE-2019-11709
- CVE-2019-11710
- CVE-2019-11711
- CVE-2019-11712
- CVE-2019-11713
- CVE-2019-11714
- CVE-2019-11715
- CVE-2019-11716
- CVE-2019-11717
- CVE-2019-11718
- CVE-2019-11719
- CVE-2019-11720
- CVE-2019-11721
- CVE-2019-11723
- CVE-2019-11724
- CVE-2019-11725
- CVE-2019-11727
- CVE-2019-11728
- CVE-2019-11729
- CVE-2019-11730
- CVE-2019-11733
- CVE-2019-11734
- CVE-2019-11735
- CVE-2019-11736
- CVE-2019-11737
- CVE-2019-11738
- CVE-2019-11740
- CVE-2019-11741
- CVE-2019-11742
- CVE-2019-11743
- CVE-2019-11744
- CVE-2019-11745
- CVE-2019-11746
- CVE-2019-11747
- CVE-2019-11748
- CVE-2019-11749
- CVE-2019-11750
- CVE-2019-11751
- CVE-2019-11752
- CVE-2019-11753
- CVE-2019-11754
- CVE-2019-11756
- CVE-2019-11757
- CVE-2019-11758
- CVE-2019-11759
- CVE-2019-11760
- CVE-2019-11761
- CVE-2019-11762
- CVE-2019-11763
- CVE-2019-11764
- CVE-2019-11765
- CVE-2019-17000
- CVE-2019-17001
- CVE-2019-17002
- CVE-2019-17005
- CVE-2019-17008
- CVE-2019-17009
- CVE-2019-17010

- CVE-2019-17011
- CVE-2019-17012
- CVE-2019-17013
- CVE-2019-17014
- CVE-2019-17015
- CVE-2019-17016
- CVE-2019-17017
- CVE-2019-17018
- CVE-2019-17019
- CVE-2019-17020
- CVE-2019-17021
- CVE-2019-17022
- CVE-2019-17023
- CVE-2019-17024
- CVE-2019-17025
- CVE-2019-17026
- CVE-2019-25136
- CVE-2019-9788
- CVE-2019-9789
- CVE-2019-9790
- CVE-2019-9791
- CVE-2019-9792
- CVE-2019-9793
- CVE-2019-9794
- CVE-2019-9795
- CVE-2019-9796
- CVE-2019-9797
- CVE-2019-9798
- CVE-2019-9799
- CVE-2019-9800
- CVE-2019-9801
- CVE-2019-9802
- CVE-2019-9803
- CVE-2019-9804
- CVE-2019-9805
- CVE-2019-9806
- CVE-2019-9807
- CVE-2019-9808
- CVE-2019-9809
- CVE-2019-9810
- CVE-2019-9811
- CVE-2019-9812
- CVE-2019-9813
- CVE-2019-9814
- CVE-2019-9815
- CVE-2019-9816
- CVE-2019-9817
- CVE-2019-9818
- CVE-2019-9819
- CVE-2019-9820
- CVE-2019-9821
- CVE-2020-12387
- CVE-2020-12388
- CVE-2020-12389
- CVE-2020-12390
- CVE-2020-12391
- CVE-2020-12392
- CVE-2020-12393
- CVE-2020-12394
- CVE-2020-12395
- CVE-2020-12396
- CVE-2020-12399
- CVE-2020-12400
- CVE-2020-12401
- CVE-2020-12402
- CVE-2020-12405
- CVE-2020-12406
- CVE-2020-12407
- CVE-2020-12408
- CVE-2020-12409
- CVE-2020-12410
- CVE-2020-12411
- CVE-2020-12412
- CVE-2020-12413
- CVE-2020-12415
- CVE-2020-12416
- CVE-2020-12417
- CVE-2020-12418
- CVE-2020-12419
- CVE-2020-12420
- CVE-2020-12421
- CVE-2020-12422
- CVE-2020-12423
- CVE-2020-12424
- CVE-2020-12425

- CVE-2020-12426
- CVE-2020-15647
- CVE-2020-15648
- CVE-2020-15652
- CVE-2020-15653
- CVE-2020-15654
- CVE-2020-15655
- CVE-2020-15656
- CVE-2020-15657
- CVE-2020-15658
- CVE-2020-15659
- CVE-2020-15663
- CVE-2020-15664
- CVE-2020-15665
- CVE-2020-15666
- CVE-2020-15667
- CVE-2020-15668
- CVE-2020-15670
- CVE-2020-15671
- CVE-2020-15673
- CVE-2020-15674
- CVE-2020-15675
- CVE-2020-15676
- CVE-2020-15677
- CVE-2020-15678
- CVE-2020-15680
- CVE-2020-15681
- CVE-2020-15682
- CVE-2020-15683
- CVE-2020-15684
- CVE-2020-16012
- CVE-2020-26950
- CVE-2020-26951
- CVE-2020-26952
- CVE-2020-26953
- CVE-2020-26954
- CVE-2020-26955
- CVE-2020-26956
- CVE-2020-26957
- CVE-2020-26958
- CVE-2020-26959
- CVE-2020-26960
- CVE-2020-26961
- CVE-2020-26962
- CVE-2020-26963
- CVE-2020-26964
- CVE-2020-26965
- CVE-2020-26966
- CVE-2020-26967
- CVE-2020-26968
- CVE-2020-26969
- CVE-2020-26971
- CVE-2020-26972
- CVE-2020-26973
- CVE-2020-26974
- CVE-2020-26975
- CVE-2020-26976
- CVE-2020-26977
- CVE-2020-26978
- CVE-2020-26979
- CVE-2020-35111
- CVE-2020-35112
- CVE-2020-35113
- CVE-2020-35114
- CVE-2020-6796
- CVE-2020-6797
- CVE-2020-6798
- CVE-2020-6799
- CVE-2020-6800
- CVE-2020-6801
- CVE-2020-6805
- CVE-2020-6806
- CVE-2020-6807
- CVE-2020-6808
- CVE-2020-6809
- CVE-2020-6810
- CVE-2020-6811
- CVE-2020-6812
- CVE-2020-6813
- CVE-2020-6814
- CVE-2020-6815
- CVE-2020-6819
- CVE-2020-6820
- CVE-2020-6821
- CVE-2020-6822

- CVE-2020-6823
- CVE-2020-6824
- CVE-2020-6825
- CVE-2020-6826
- CVE-2020-6829
- CVE-2020-6831
- CVE-2021-23953
- CVE-2021-23954
- CVE-2021-23955
- CVE-2021-23956
- CVE-2021-23957
- CVE-2021-23958
- CVE-2021-23959
- CVE-2021-23960
- CVE-2021-23961
- CVE-2021-23962
- CVE-2021-23963
- CVE-2021-23964
- CVE-2021-23965
- CVE-2021-23968
- CVE-2021-23969
- CVE-2021-23970
- CVE-2021-23971
- CVE-2021-23972
- CVE-2021-23973
- CVE-2021-23974
- CVE-2021-23975
- CVE-2021-23976
- CVE-2021-23977
- CVE-2021-23978
- CVE-2021-23979
- CVE-2021-23981
- CVE-2021-23982
- CVE-2021-23983
- CVE-2021-23984
- CVE-2021-23985
- CVE-2021-23986
- CVE-2021-23987
- CVE-2021-23988
- CVE-2021-23994
- CVE-2021-23995
- CVE-2021-23996
- CVE-2021-23997
- CVE-2021-23998
- CVE-2021-23999
- CVE-2021-24000
- CVE-2021-24001
- CVE-2021-24002
- CVE-2021-29944
- CVE-2021-29945
- CVE-2021-29946
- CVE-2021-29947
- CVE-2021-29951
- CVE-2021-29952
- CVE-2021-29953
- CVE-2021-29955
- CVE-2021-29959
- CVE-2021-29960
- CVE-2021-29961
- CVE-2021-29962
- CVE-2021-29963
- CVE-2021-29964
- CVE-2021-29965
- CVE-2021-29966
- CVE-2021-29967
- CVE-2021-29968
- CVE-2021-29970
- CVE-2021-29971
- CVE-2021-29972
- CVE-2021-29973
- CVE-2021-29974
- CVE-2021-29975
- CVE-2021-29976
- CVE-2021-29977
- CVE-2021-29980
- CVE-2021-29981
- CVE-2021-29982
- CVE-2021-29983
- CVE-2021-29984
- CVE-2021-29985
- CVE-2021-29986
- CVE-2021-29987
- CVE-2021-29988
- CVE-2021-29989
- CVE-2021-29990

- CVE-2021-29991
- CVE-2021-29993
- CVE-2021-30547
- CVE-2021-38491
- CVE-2021-38492
- CVE-2021-38493
- CVE-2021-38494
- CVE-2021-38496
- CVE-2021-38497
- CVE-2021-38498
- CVE-2021-38499
- CVE-2021-38500
- CVE-2021-38501
- CVE-2021-38503
- CVE-2021-38504
- CVE-2021-38505
- CVE-2021-38506
- CVE-2021-38507
- CVE-2021-38508
- CVE-2021-38509
- CVE-2021-38510
- CVE-2021-4128
- CVE-2021-4129
- CVE-2021-4140
- CVE-2021-4221
- CVE-2021-43530
- CVE-2021-43531
- CVE-2021-43532
- CVE-2021-43533
- CVE-2021-43534
- CVE-2021-43535
- CVE-2021-43536
- CVE-2021-43537
- CVE-2021-43538
- CVE-2021-43539
- CVE-2021-43540
- CVE-2021-43541
- CVE-2021-43542
- CVE-2021-43543
- CVE-2021-43544
- CVE-2021-43545
- CVE-2021-43546
- CVE-2022-0511
- CVE-2022-0843
- CVE-2022-1097
- CVE-2022-1529
- CVE-2022-1802
- CVE-2022-1887
- CVE-2022-2200
- CVE-2022-22736
- CVE-2022-22737
- CVE-2022-22738
- CVE-2022-22739
- CVE-2022-22740
- CVE-2022-22741
- CVE-2022-22742
- CVE-2022-22743
- CVE-2022-22744
- CVE-2022-22745
- CVE-2022-22746
- CVE-2022-22747
- CVE-2022-22748
- CVE-2022-22749
- CVE-2022-22750
- CVE-2022-22751
- CVE-2022-22752
- CVE-2022-22753
- CVE-2022-22754
- CVE-2022-22755
- CVE-2022-22756
- CVE-2022-22757
- CVE-2022-22758
- CVE-2022-22759
- CVE-2022-22760
- CVE-2022-22761
- CVE-2022-22762
- CVE-2022-22763
- CVE-2022-22764
- CVE-2022-2505
- CVE-2022-26381
- CVE-2022-26382
- CVE-2022-26383
- CVE-2022-26384
- CVE-2022-26385
- CVE-2022-26387

- CVE-2022-26485
- CVE-2022-26486
- CVE-2022-28281
- CVE-2022-28282
- CVE-2022-28283
- CVE-2022-28284
- CVE-2022-28285
- CVE-2022-28286
- CVE-2022-28287
- CVE-2022-28288
- CVE-2022-28289
- CVE-2022-29909
- CVE-2022-29910
- CVE-2022-29911
- CVE-2022-29912
- CVE-2022-29914
- CVE-2022-29915
- CVE-2022-29916
- CVE-2022-29917
- CVE-2022-29918
- CVE-2022-31736
- CVE-2022-31737
- CVE-2022-31738
- CVE-2022-31739
- CVE-2022-31740
- CVE-2022-31741
- CVE-2022-31742
- CVE-2022-31743
- CVE-2022-31744
- CVE-2022-31745
- CVE-2022-31746
- CVE-2022-31747
- CVE-2022-31748
- CVE-2022-3266
- CVE-2022-34468
- CVE-2022-34469
- CVE-2022-34470
- CVE-2022-34471
- CVE-2022-34472
- CVE-2022-34473
- CVE-2022-34474
- CVE-2022-34475
- CVE-2022-34476
- CVE-2022-34477
- CVE-2022-34478
- CVE-2022-34479
- CVE-2022-34480
- CVE-2022-34481
- CVE-2022-34482
- CVE-2022-34483
- CVE-2022-34484
- CVE-2022-34485
- CVE-2022-36314
- CVE-2022-36315
- CVE-2022-36316
- CVE-2022-36317
- CVE-2022-36318
- CVE-2022-36319
- CVE-2022-36320
- CVE-2022-38472
- CVE-2022-38473
- CVE-2022-38474
- CVE-2022-38475
- CVE-2022-38477
- CVE-2022-38478
- CVE-2022-40956
- CVE-2022-40957
- CVE-2022-40958
- CVE-2022-40959
- CVE-2022-40960
- CVE-2022-40961
- CVE-2022-40962
- CVE-2022-42927
- CVE-2022-42928
- CVE-2022-42929
- CVE-2022-42930
- CVE-2022-42931
- CVE-2022-42932
- CVE-2022-45403
- CVE-2022-45404
- CVE-2022-45405
- CVE-2022-45406
- CVE-2022-45407
- CVE-2022-45408
- CVE-2022-45409

- CVE-2022-45410
- CVE-2022-45411
- CVE-2022-45412
- CVE-2022-45413
- CVE-2022-45415
- CVE-2022-45416
- CVE-2022-45417
- CVE-2022-45418
- CVE-2022-45419
- CVE-2022-45420
- CVE-2022-45421
- CVE-2022-46871
- CVE-2022-46872
- CVE-2022-46873
- CVE-2022-46874
- CVE-2022-46875
- CVE-2022-46877
- CVE-2022-46878
- CVE-2022-46879
- CVE-2022-46880
- CVE-2022-46881
- CVE-2022-46882
- CVE-2022-46883
- CVE-2022-46884
- CVE-2022-46885
- CVE-2023-0767
- CVE-2023-23597
- CVE-2023-23598
- CVE-2023-23599
- CVE-2023-23600
- CVE-2023-23601
- CVE-2023-23602
- CVE-2023-23603
- CVE-2023-23604
- CVE-2023-23605
- CVE-2023-23606
- CVE-2023-25728
- CVE-2023-25729
- CVE-2023-25730
- CVE-2023-25731
- CVE-2023-25732
- CVE-2023-25733
- CVE-2023-25734
- CVE-2023-25735
- CVE-2023-25736
- CVE-2023-25737
- CVE-2023-25738
- CVE-2023-25739
- CVE-2023-25740
- CVE-2023-25741
- CVE-2023-25742
- CVE-2023-25743
- CVE-2023-25744
- CVE-2023-25745
- CVE-2023-25747
- CVE-2023-25748
- CVE-2023-25749
- CVE-2023-25750
- CVE-2023-25751
- CVE-2023-25752
- CVE-2023-28159
- CVE-2023-28160
- CVE-2023-28161
- CVE-2023-28162
- CVE-2023-28163
- CVE-2023-28164
- CVE-2023-28176
- CVE-2023-28177
- CVE-2023-29531
- CVE-2023-29532
- CVE-2023-29533
- CVE-2023-29534
- CVE-2023-29535
- CVE-2023-29536
- CVE-2023-29537
- CVE-2023-29538
- CVE-2023-29539
- CVE-2023-29540
- CVE-2023-29541
- CVE-2023-29542
- CVE-2023-29543
- CVE-2023-29544
- CVE-2023-29545
- CVE-2023-29546
- CVE-2023-29547

- CVE-2023-29548
- CVE-2023-29549
- CVE-2023-29550
- CVE-2023-29551
- CVE-2023-32205
- CVE-2023-32206
- CVE-2023-32207
- CVE-2023-32208
- CVE-2023-32209
- CVE-2023-32210
- CVE-2023-32211
- CVE-2023-32212
- CVE-2023-32213
- CVE-2023-32214
- CVE-2023-32215
- CVE-2023-32216
- CVE-2023-34414
- CVE-2023-34415
- CVE-2023-34416
- CVE-2023-34417
- CVE-2023-3482
- CVE-2023-3600
- CVE-2023-37201
- CVE-2023-37202
- CVE-2023-37203
- CVE-2023-37204
- CVE-2023-37205
- CVE-2023-37206
- CVE-2023-37207
- CVE-2023-37208
- CVE-2023-37209
- CVE-2023-37210
- CVE-2023-37211
- CVE-2023-37212
- CVE-2023-37455
- CVE-2023-37456
- CVE-2023-4045
- CVE-2023-4046
- CVE-2023-4047
- CVE-2023-4048
- CVE-2023-4049
- CVE-2023-4050
- CVE-2023-4051
- CVE-2023-4052
- CVE-2023-4053
- CVE-2023-4054
- CVE-2023-4055
- CVE-2023-4056
- CVE-2023-4057
- CVE-2023-4058
- CVE-2023-4573
- CVE-2023-4574
- CVE-2023-4575
- CVE-2023-4576
- CVE-2023-4577
- CVE-2023-4578
- CVE-2023-4579
- CVE-2023-4580
- CVE-2023-4581
- CVE-2023-4582
- CVE-2023-4583
- CVE-2023-4584
- CVE-2023-4585
- CVE-2023-4863
- CVE-2023-49060
- CVE-2023-49061
- CVE-2023-5168
- CVE-2023-5169
- CVE-2023-5170
- CVE-2023-5171
- CVE-2023-5172
- CVE-2023-5173
- CVE-2023-5174
- CVE-2023-5175
- CVE-2023-5176
- CVE-2023-5217
- CVE-2023-5388
- CVE-2023-5721
- CVE-2023-5722
- CVE-2023-5723
- CVE-2023-5724
- CVE-2023-5725
- CVE-2023-5726
- CVE-2023-5727
- CVE-2023-5728

- CVE-2023-5729
- CVE-2023-5730
- CVE-2023-5731
- CVE-2023-5732
- CVE-2023-5758
- CVE-2023-6135
- CVE-2023-6204
- CVE-2023-6205
- CVE-2023-6206
- CVE-2023-6207
- CVE-2023-6208
- CVE-2023-6209
- CVE-2023-6210
- CVE-2023-6211
- CVE-2023-6212
- CVE-2023-6213
- CVE-2023-6856
- CVE-2023-6857
- CVE-2023-6858
- CVE-2023-6859
- CVE-2023-6860
- CVE-2023-6861
- CVE-2023-6863
- CVE-2023-6864
- CVE-2023-6865
- CVE-2023-6866
- CVE-2023-6867
- CVE-2023-6868
- CVE-2023-6869
- CVE-2023-6870
- CVE-2023-6871
- CVE-2023-6872
- CVE-2023-6873
- CVE-2024-0741
- CVE-2024-0742
- CVE-2024-0743
- CVE-2024-0744
- CVE-2024-0745
- CVE-2024-0746
- CVE-2024-0747
- CVE-2024-0748
- CVE-2024-0749
- CVE-2024-0750
- CVE-2024-0751
- CVE-2024-0752
- CVE-2024-0753
- CVE-2024-0754
- CVE-2024-0755
- CVE-2024-10004
- CVE-2024-10458
- CVE-2024-10459
- CVE-2024-10460
- CVE-2024-10461
- CVE-2024-10462
- CVE-2024-10463
- CVE-2024-10464
- CVE-2024-10465
- CVE-2024-10466
- CVE-2024-10467
- CVE-2024-10468
- CVE-2024-10941
- CVE-2024-11691
- CVE-2024-11692
- CVE-2024-11693
- CVE-2024-11694
- CVE-2024-11695
- CVE-2024-11696
- CVE-2024-11697
- CVE-2024-11698
- CVE-2024-11699
- CVE-2024-11700
- CVE-2024-11701
- CVE-2024-11702
- CVE-2024-11703
- CVE-2024-11704
- CVE-2024-11705
- CVE-2024-11706
- CVE-2024-11708
- CVE-2024-1546
- CVE-2024-1547
- CVE-2024-1548
- CVE-2024-1549
- CVE-2024-1550
- CVE-2024-1551
- CVE-2024-1552

- CVE-2024-1553
- CVE-2024-1554
- CVE-2024-1555
- CVE-2024-1556
- CVE-2024-1557
- CVE-2024-2605
- CVE-2024-2606
- CVE-2024-2607
- CVE-2024-2608
- CVE-2024-2609
- CVE-2024-2610
- CVE-2024-2611
- CVE-2024-2612
- CVE-2024-2613
- CVE-2024-2614
- CVE-2024-2615
- CVE-2024-26283
- CVE-2024-29943
- CVE-2024-29944
- CVE-2024-31392
- CVE-2024-3302
- CVE-2024-38312
- CVE-2024-38313
- CVE-2024-3852
- CVE-2024-3853
- CVE-2024-3854
- CVE-2024-3855
- CVE-2024-3856
- CVE-2024-3857
- CVE-2024-3858
- CVE-2024-3859
- CVE-2024-3860
- CVE-2024-3861
- CVE-2024-3862
- CVE-2024-3863
- CVE-2024-3864
- CVE-2024-3865
- CVE-2024-43111
- CVE-2024-43112
- CVE-2024-43113
- CVE-2024-4367
- CVE-2024-4764
- CVE-2024-4765
- CVE-2024-4766
- CVE-2024-4767
- CVE-2024-4768
- CVE-2024-4769
- CVE-2024-4770
- CVE-2024-4771
- CVE-2024-4772
- CVE-2024-4773
- CVE-2024-4774
- CVE-2024-4775
- CVE-2024-4776
- CVE-2024-4777
- CVE-2024-4778
- CVE-2024-5687
- CVE-2024-5688
- CVE-2024-5689
- CVE-2024-5690
- CVE-2024-5691
- CVE-2024-5692
- CVE-2024-5693
- CVE-2024-5694
- CVE-2024-5695
- CVE-2024-5696
- CVE-2024-5697
- CVE-2024-5698
- CVE-2024-5699
- CVE-2024-5700
- CVE-2024-5701
- CVE-2024-5702
- CVE-2024-6600
- CVE-2024-6601
- CVE-2024-6602
- CVE-2024-6603
- CVE-2024-6604
- CVE-2024-6605
- CVE-2024-6606
- CVE-2024-6607
- CVE-2024-6608
- CVE-2024-6609
- CVE-2024-6610
- CVE-2024-6611
- CVE-2024-6612

- CVE-2024-6613
- CVE-2024-6614
- CVE-2024-6615
- CVE-2024-7518
- CVE-2024-7519
- CVE-2024-7520
- CVE-2024-7521
- CVE-2024-7522
- CVE-2024-7523
- CVE-2024-7524
- CVE-2024-7525
- CVE-2024-7526
- CVE-2024-7527
- CVE-2024-7528
- CVE-2024-7529
- CVE-2024-7530
- CVE-2024-7531
- CVE-2024-7652
- CVE-2024-8381
- CVE-2024-8382
- CVE-2024-8383
- CVE-2024-8384
- CVE-2024-8385
- CVE-2024-8386
- CVE-2024-8387
- CVE-2024-8388
- CVE-2024-8389
- CVE-2024-8897
- CVE-2024-8900
- CVE-2024-9391
- CVE-2024-9392
- CVE-2024-9393
- CVE-2024-9394
- CVE-2024-9395
- CVE-2024-9396
- CVE-2024-9397
- CVE-2024-9398
- CVE-2024-9399
- CVE-2024-9400
- CVE-2024-9401
- CVE-2024-9402
- CVE-2024-9403
- CVE-2024-9680
- CVE-2024-9936
- CVE-2025-0237
- CVE-2025-0238
- CVE-2025-0239
- CVE-2025-0240
- CVE-2025-0241
- CVE-2025-0242
- CVE-2025-0243
- CVE-2025-0244
- CVE-2025-0245
- CVE-2025-0246
- CVE-2025-0247
- CVE-2025-1009
- CVE-2025-1010
- CVE-2025-1011
- CVE-2025-1012
- CVE-2025-1013
- CVE-2025-1014
- CVE-2025-1016
- CVE-2025-1017
- CVE-2025-1018
- CVE-2025-1019
- CVE-2025-1020
- mozilla products -- spoofing attack
- mozilla -- multiple vulnerabilities
- Exploit for Insufficient Verification of Data Authenticity in Rarlab Winrar
- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for Type Confusion in Mozilla Thunderbird
- Exploit for Improper Restriction of Operations within the Bounds of a Memory Buffer in Mozilla Firefox
- mozilla -- multiple vulnerabilities
- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for NULL Pointer Dereference in Gpac
- Spidermonkey - IonMonkey Type Inference is Incorrect for Constructors Entered via OSR
- SpiderMonkey - IonMonkey Compiled Code Fails to Update Inferred Property Types (Type Confusion)
- Spidermonkey - IonMonkey Leaks JS_OPTIMIZED_OUT Magic Value to Script
- Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack
- Firefox 72 IonMonkey - JIT Type Confusion
- Mozilla Firefox 67 - Array.pop JIT Type Confusion
- Spidermonkey - IonMonkey Leaks JS_OPTIMIZED_OUT Magic Value to Script
- Spidermonkey - IonMonkey Type Inference is Incorrect for Constructors Entered via OSR
- Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack
- SpiderMonkey - IonMonkey Compiled Code Fails to Update Inferred Property Types (Type Confusion)

- Exploit for Out-of-bounds Write in Google Chrome
- Exploit for CVE-2024-29943
- Exploit for Improper Input Validation in Mozilla Firefox Esr
- Exploit for Out-of-bounds Write in Google Chrome
- Security vulnerabilities fixed in Firefox 62 — Mozilla
- Security vulnerabilities fixed in Firefox 62.0.2 — Mozilla
- Security vulnerabilities fixed in Firefox 62.0.3 and Firefox ESR 60.2.2 — Mozilla
- Security vulnerabilities fixed in Firefox 63 — Mozilla
- Security vulnerabilities fixed in Firefox 64 — Mozilla
- Security vulnerabilities fixed in Firefox 65 — Mozilla
- Security vulnerabilities fixed in Firefox 65.0.1 — Mozilla
- Security vulnerabilities fixed in Firefox 66 — Mozilla
- Security vulnerabilities fixed in Firefox 66.0.1 — Mozilla
- Security vulnerabilities fixed in Firefox 67 — Mozilla
- Security vulnerabilities fixed in Firefox 67.0.2 — Mozilla
- Security vulnerabilities fixed in Firefox 67.0.3 and Firefox ESR 60.7.1 — Mozilla
- Security vulnerabilities fixed in Firefox 67.0.4 and Firefox ESR 60.7.2 — Mozilla
- Security vulnerabilities fixed in Firefox 68 — Mozilla
- Stored passwords in 'Saved Logins' can be copied without master password entry — Mozilla
- Security vulnerabilities fixed in Firefox 69 — Mozilla
- Security vulnerabilities fixed in Firefox 69.0.1 — Mozilla
- Security vulnerabilities fixed in - Firefox 70 — Mozilla
- Security Vulnerabilities fixed in - Firefox 71 — Mozilla
- Security Vulnerabilities fixed in Firefox 72 — Mozilla
- Security Vulnerabilities fixed in Firefox 72.0.1 and Firefox ESR 68.4.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 73 — Mozilla
- Security Vulnerabilities fixed in Firefox 74 — Mozilla
- Security Vulnerabilities fixed in Firefox 74.0.1 and Firefox ESR 68.6.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 75 — Mozilla
- Security Vulnerabilities fixed in Firefox 76 — Mozilla
- Security Vulnerabilities fixed in Firefox 77 — Mozilla
- Security Vulnerabilities fixed in Firefox 78 — Mozilla
- Security Vulnerabilities fixed in Firefox for Android 68.10.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 78.0.2 — Mozilla
- Security Vulnerabilities fixed in Firefox 79 — Mozilla
- Security Vulnerabilities fixed in Firefox 80 — Mozilla
- Security Vulnerabilities fixed in Firefox 81 — Mozilla
- Security Vulnerabilities fixed in Firefox 82 — Mozilla
- Security Vulnerabilities fixed in Firefox 82.0.3, Firefox ESR 78.4.1, and Thunderbird 78.4.2 — Mozilla
- Security Vulnerabilities fixed in Firefox 83 — Mozilla
- Security Vulnerabilities fixed in Firefox 84 — Mozilla
- Security Vulnerabilities fixed in Firefox 84.0.2, Firefox for Android 84.1.3, and Firefox ESR 78.6.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 85 — Mozilla
- Security Vulnerabilities fixed in Firefox 85.0.1 and Firefox ESR 78.7.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 86 — Mozilla
- Security Vulnerabilities fixed in Firefox 87 — Mozilla
- Security Vulnerabilities fixed in Firefox 88 — Mozilla
- Security Vulnerabilities fixed in Firefox 88.0.1, Firefox for Android 88.1.3 — Mozilla
- Security Vulnerabilities fixed in Firefox 89 — Mozilla
- Security Vulnerabilities fixed in Firefox 89.0.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 90 — Mozilla
- Security Vulnerabilities fixed in Firefox 91 — Mozilla
- Security Vulnerabilities fixed in Firefox 91.0.1 and Thunderbird 91.0.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 92 — Mozilla
- Security Vulnerabilities fixed in Firefox 93 — Mozilla
- Security Vulnerabilities fixed in Firefox 94 — Mozilla
- Security Vulnerabilities fixed in Firefox 95 — Mozilla
- Security Vulnerabilities fixed in Firefox 96 — Mozilla
- Security Vulnerabilities fixed in Firefox 97 — Mozilla
- Security Vulnerabilities fixed in Firefox 97.0.2, Firefox ESR 91.6.1, Firefox for Android 97.3.0, and Focus 97.3.0 — Mozilla
- Security Vulnerabilities fixed in Firefox 98 — Mozilla
- Security Vulnerabilities fixed in Firefox 99 — Mozilla
- Security Vulnerabilities fixed in Firefox 100 — Mozilla
- Security Vulnerabilities fixed in Firefox 100.0.2, Firefox for Android 100.3.0, Firefox ESR 91.9.1, Thunderbird 91.9.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 101 — Mozilla
- Security Vulnerabilities fixed in Firefox 102 — Mozilla
- Security Vulnerabilities fixed in Firefox 103 — Mozilla
- Security Vulnerabilities fixed in Firefox 104 — Mozilla
- Security Vulnerabilities fixed in Firefox 105 — Mozilla
- Security Vulnerabilities fixed in Firefox 106 — Mozilla
- Security Vulnerabilities fixed in Firefox 107 — Mozilla
- Security Vulnerabilities fixed in Firefox 108 — Mozilla
- Security Vulnerabilities fixed in Firefox 109 — Mozilla
- Security Vulnerabilities fixed in Firefox 110 — Mozilla
- Security Vulnerabilities fixed in Firefox 111 — Mozilla
- Security Vulnerabilities fixed in Firefox 112, Firefox for Android 112, Focus for Android 112 — Mozilla
- Security Vulnerabilities fixed in Firefox 113 — Mozilla
- Security Vulnerabilities fixed in Firefox 114 — Mozilla
- Security Vulnerabilities fixed in Firefox 115 — Mozilla
- Security Vulnerabilities fixed in Firefox 115.0.2 and Firefox ESR 115.0.2 — Mozilla
- Security Vulnerabilities fixed in Firefox 116 — Mozilla
- Security Vulnerabilities fixed in Firefox 117 — Mozilla
- Security Vulnerability fixed in Firefox 117.0.1, Firefox ESR 115.2.1, Firefox ESR 102.15.1, Thunderbird 102.15.1, and Thunderbird 115.2.2 — Mozilla
- Security Vulnerabilities fixed in Firefox 118 — Mozilla
- Security Vulnerability fixed in Firefox 118.0.1, Firefox ESR 115.3.1, Firefox for Android 118.1.0, Firefox Focus for Android 118.1.0, and Thunderbird 115.3.1. — Mozilla

- Security Vulnerabilities fixed in Firefox 119 — Mozilla
- Security Vulnerabilities fixed in Firefox 120 — Mozilla
- Security Vulnerabilities fixed in Firefox 121 — Mozilla
- Security Vulnerabilities fixed in Firefox 122 — Mozilla
- Security Vulnerabilities fixed in Firefox 123 — Mozilla
- Security Vulnerabilities fixed in Firefox 124 — Mozilla
- Security Vulnerabilities fixed in Firefox 124.0.1 — Mozilla
- Security Vulnerabilities fixed in Firefox 125 — Mozilla
- Security Vulnerabilities fixed in Firefox 126 — Mozilla
- Security Vulnerabilities fixed in Firefox 127 — Mozilla
- Security Vulnerabilities fixed in Firefox 128 — Mozilla
- Security Vulnerabilities fixed in Firefox 129 — Mozilla
- Security Vulnerabilities fixed in Firefox 130 — Mozilla
- Security Vulnerabilities fixed in Firefox 131 — Mozilla
- Security Vulnerability fixed in Firefox 131.0.2, Firefox ESR 128.3.1, Firefox ESR 115.16.1 — Mozilla
- Security Vulnerability fixed in Firefox 131.0.3 — Mozilla
- Security Vulnerabilities fixed in Firefox 132 — Mozilla
- Security Vulnerabilities fixed in Firefox 133 — Mozilla
- Security Vulnerabilities fixed in Firefox 134 — Mozilla
- Security Vulnerabilities fixed in Firefox 135 — Mozilla
- Firefox MCallGetProperty Write Side Effects Use After Free Exploit
- Firefox Array.prototype.slice Buffer Overflow
- SpiderMonkey IonMonkey Type Confusion
- SpiderMonkey IonMonkey Type Confusion
- Spidermonkey IonMonkey JS_OPTIMIZED_OUT Value Leak
- Spidermonkey IonMonkey Incorrect Prediction
- Firefox 72 IonMonkey JIT Type Confusion
- Mozilla Firefox 67 Array.pop JIT Type Confusion
- Firefox MCallGetProperty Write Side Effects Use-After-Free
- A Pwn2Own SpiderMonkey JIT Bug