

Data Bank of Information Security Threats

[home \(/\)](#) / [List of vulnerabilities](#)

Withdraw by: 10, 20 (</vul?size=20>) , 50 (</vul?size=50>) , 100 (</vul?size=100>) Sorting:▼

BDU:2023-06302
(</vul/2023-06302>) Protected information disclosure vulnerability in the WebKitGTK and WPE WebKit web page rendering modules, which could allow an attacker to disclose protected information

BDU:2023-06301
(</vul/2023-06301>) A vulnerability in the Application Quality of Experience (AppQoE) and Unified Threat Defense (UTD) components of the Cisco IOS XE operating system that allows an attacker to cause a denial of service

BDU:2023-06300
(</vul/2023-06300>) A vulnerability in the web interface of the Cisco IOS XE operating system allows an attacker to execute arbitrary commands

BDU:2023-06299
(</vul/2023-06299>) A vulnerability in the Extensions component of the Google Chrome browser that allows an attacker to execute arbitrary code

BDU:2023-06298
(</vul/2023-06298>) A vulnerability in the Passwords component of the Google Chrome browser that allows an attacker to execute arbitrary code

BDU:2023-06297
(</vul/2023-06297>) A vulnerability in the program/lib/Roundcube/rcube_string_replacer.php component of the RoundCube Webmail email client, which allows an attacker to conduct a cross-site scripting attack

BDU:2023-06296
(</vul/2023-06296>) A vulnerability in the centralized endpoint security management tool WithSecure Policy Manager due to insufficient input validation that could allow an attacker to execute arbitrary code

BDU:2023-06295
(/vul/2023-06295) A stack-based buffer overflow vulnerability in the Gstreamer multimedia framework could allow an attacker to execute arbitrary code.

BDU:2023-06294
(/vul/2023-06294) An integer overflow vulnerability in the Gstreamer multimedia framework could allow an attacker to execute arbitrary code.

BDU:2023-06293
(/vul/2023-06293) A vulnerability in the OPTEE component of the firmware of MediaTek chips, which allows an attacker to escalate their privileges

<< (/vul)	< (/vul)	1 (/vul)	2 (/vul?page=2)	3 (/vul?page=3)	4 (/vul?page=4)	5 (/vul?page=5)	6 (/vul?page=6)
7 (/vul?page=7)	8 (/vul?page=8)	9 (/vul?page=9)	10 (/vul?page=10)	> (/vul?page=2)	>> (/vul?page=5059)		

[Download vulnerability information in XLSX format \(/files/documents/vulldist.xlsx\)](/files/documents/vulldist.xlsx)

[Download vulnerability information in XML format \(test version\) \(/files/documents/vulxml.zip\)](/files/documents/vulxml.zip)

FILTRATION

Contextual search by vulnerability name

Software Manufacturer 

Select software manufacturer

Software type 

Select software type

Software 

Select software

Hardware platform 

Select platform

Software version 

Select software version

Vulnerability status ?

Select vulnerability status

▼ Add. options

Date range ?

c

By

☐ Vulnerabilities associated with information security incidents ?

Year added ?

Select year added

Vulnerability class ?

Select vulnerability class

Danger level ?

Select vulnerability severity level

Base vector ?

AV

A.C.

Au

C

I

A

Error type ID ?

Доступен множественный выбор

Other identification systems ?

Select ID

Availability of exploit

Select value

Method of operation ?

Select value

Remedy ?

Select value

operating system ?

Select OS

Reset

Apply

LAST CHANGES

10/04/2023

Protected information disclosure vulnerability in the WebKitGTK and WPE WebKit web page rendering modules, which could allow an attacker to disclose protected information (/vul/2023-06302)

10/04/2023

A vulnerability in the Application Quality of Experience (AppQoE) and Unified Threat Defense (UTD) components of the Cisco IOS XE operating system that allows an attacker to cause a denial of service (/vul/2023-06301)

10/04/2023

A vulnerability in the web interface of the Cisco IOS XE operating system allows an attacker to execute arbitrary commands (/vul/2023-06300)

10/04/2023

A vulnerability in the Extensions component of the Google Chrome browser that allows an attacker to execute arbitrary code (/vul/2023-06299)

10/04/2023

A vulnerability in the Passwords component of the Google Chrome browser that allows an attacker to execute arbitrary code (/vul/2023-06298)

10/04/2023

A vulnerability in the program/lib/Roundcube/rcube_string_replacer.php component of the RoundCube Webmail email client, which allows an attacker to conduct a cross-site scripting attack (/vul/2023-06297)

10/04/2023

A vulnerability in the centralized endpoint security management tool WithSecure Policy Manager due to insufficient input validation that could allow an attacker to execute arbitrary code (/vul/2023-06296)

10/04/2023

A stack-based buffer overflow vulnerability in the Gstreamer multimedia framework could allow an attacker to execute arbitrary code. (/vul/2023-06295)

10/04/2023

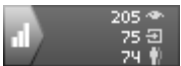
An integer overflow vulnerability in the Gstreamer multimedia framework could allow an attacker to execute arbitrary code. (/vul/2023-06294)

10/04/2023

A vulnerability in the OPTEE component of the firmware of MediaTek chips, which allows an attacker to escalate their privileges (/vul/2023-06293)

Threats: 222 Vulnerabilities: 50586 Last update: 10/04/2023

© FAU "GNIIII PTZI FSTEC of Russia"



([https://metrika.yandex.ru/stat/?](https://metrika.yandex.ru/stat/?id=28243701&from=informer)

id=28243701&from=informer)