BULLETIN (SB21-270)

VULNERABILITY SUMMARY FOR THE WEEK OF

23RD SEPTEMBER, 2021

Bulletin (SB21-270)
Vulnerability Summary for the Week of September 23, 2021

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.
The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.
Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -
Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .
The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zohocorp -- manageengine_adselfservice_plus	Zoho ManageEngine ADSelfService Plus 6111 and prior is vulnerable to SQL Injection while linking the databases.	2021-09-10	7.5	CVE-2021-37422
zohocorp -- manageengine_adselfservice_plus	Zoho ManageEngine ADSelfService Plus 6111 and prior is vulnerable to linked applications takeover.	2021-09-10	7.5	CVE-2021-37423
adaptivescale -- lxdui	A Hardcoded JWT Secret Key in metadata.py in AdaptiveScale LXDUI through 2.1.3 allows attackers to gain admin access to the host system.	2021-09-03	10	CVE-2021-40494
arubanetworks -- arubaos	A remote arbitrary command execution vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.16. Aruba has released patches for ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37724
arubanetworks -- arubaos	A remote arbitrary command execution vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.16. Aruba has released patches for ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37723
arubanetworks -- sd-wan	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37718
arubanetworks -- sd-wan	A remote buffer overflow vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	7.5	CVE-2021-37716
arubanetworks -- sd-wan	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37717
arubanetworks -- sd-wan	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37722
arubanetworks -- sd-wan	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37721
arubanetworks -- sd-wan	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37720
arubanetworks -- sd-wan	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	9	CVE-2021-37719
bluecms_project -- bluecms	BlueCMS v1.6 contains a SQL injection vulnerability via /ad_js.php.	2021-09-08	7.5	CVE-2020-19853
espressif -- esp-idf	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly restrict the Feature Page upon reception of an LMP Feature Response Extended packet, allowing attackers in radio range to trigger arbitrary code execution in ESP32 via a crafted Extended Features bitfield payload.	2021-09-07	8.3	CVE-2021-28139
moxa -- wac-2004_firmware	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP-323-JP-CT-T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	2021-09-07	9	CVE-2021-39279
simple_water_refilling_station_management_system_project -- simple_water_refil	SQL Injection can occur in Simple Water Refilling Station Management System 1.0 via the water_refilling/classes/Login.php username parameter.	2021-09-07	7.5	CVE-2021-38840

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ling_station_management_system				
sketch -- sketch	Sketch before 75 mishandles external library feeds.	2021-09-06	7.5	CVE-2021-40531
telegram -- web_k_alpha	Telegram Web K Alpha before 0.7.2 mishandles the characters in a document extension.	2021-09-06	7.5	CVE-2021-40532
ulfius_project -- ulfius	ulfius_uri_logger in Ulfius HTTP Framework before 2.7.4 omits con_info initialization and a con_info->request NULL check for certain malformed HTTP requests.	2021-09-07	7.5	CVE-2021-40540

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function config_input in libavfilter/vf_gblur.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20891
ffmpeg -- ffmpeg	Integer Overflow vulnerability in function filter16_prewitt in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20898
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function gaussian_blur in libavfilter/vf_edgedetect.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20900
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function filter_slice in libavfilter/vf_bm3d.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20897
ffmpeg -- ffmpeg	An issue was discovered in function latm_write_packet in libavformat/latmenc.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts due to a Null pointer dereference.	2021-09-20	6.8	CVE-2020-20896
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function filter_vertically_##name in libavfilter/vf_avgblur.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20895
ffmpeg -- ffmpeg	An issue was discovered in function filter_frame in libavfilter/vf_lenscorrection.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts due to a division by zero.	2021-09-20	6.8	CVE-2020-20892
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function activate in libavfilter/af_afade.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20893
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function gaussian_blur in libavfilter/vf_edgedetect.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20894
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function config_props in libavfilter/vf_bwdif.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20899
ffmpeg -- ffmpeg	Integer Overflow vulnerability in function filter_prewitt in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2021-38092
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function filter_frame in libavfilter/vf_fieldorder.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2020-20901
ffmpeg -- ffmpeg	Buffer Overflow vulnerability in function config_input in libavfilter/vf_bm3d.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2021-38089
ffmpeg -- ffmpeg	Integer Overflow vulnerability in function filter16_roberts in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2021-38090
ffmpeg -- ffmpeg	Integer Overflow vulnerability in function filter16_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2021-38091

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ffmpeg -- ffmpeg	Integer Overflow vulnerability in function filter_robert in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2021-38093
ffmpeg -- ffmpeg	Integer Overflow vulnerability in function filter_sobel in libavfilter/vf_convolution.c in Ffmpeg 4.2.1, allows attackers to cause a Denial of Service or other unspecified impacts.	2021-09-20	6.8	CVE-2021-38094
gnu -- libredwg	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function check_POLYLINE_handles() located in decode.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39523
gnu -- libredwg	An issue was discovered in libredwg through v0.10.1.3751. appinfo_private() in decode.c has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39527
gnu -- libredwg	An issue was discovered in libredwg through v0.10.1.3751. A NULL pointer dereference exists in the function bit_read_BB() located in bits.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39521
gnu -- libredwg	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2nlen() in bits.c has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39530
gnu -- libredwg	An issue was discovered in libredwg through v0.10.1.3751. bit_wcs2len() in bits.c has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39522
gnu -- libredwg	An issue was discovered in libredwg through v0.10.1.3751. bit_read_fixed() in bits.c has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39525
gnu -- libredwg	An issue was discovered in libredwg through v0.10.1.3751. dwg_free_MATERIAL_private() in dwg.spec has a double free.	2021-09-20	6.8	CVE-2021-39528
jpeg -- libjpeg	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function SampleInterleavedLSScan::ParseMCU() located in sampleinterleavedlsscan.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39515
jpeg -- libjpeg	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::PushReconstructedData() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39520
jpeg -- libjpeg	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::PullQData() located in blockbitmaprequester.cpp It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39519
jpeg -- libjpeg	An issue was discovered in libjpeg through 2020021. LineBuffer::FetchRegion() in linebuffer.cpp has a heap-based buffer overflow.	2021-09-20	4.3	CVE-2021-39518
jpeg -- libjpeg	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function BlockBitmapRequester::ReconstructUnsampled() located in blockbitmaprequester.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39517
jpeg -- libjpeg	An issue was discovered in libjpeg through 2020021. A NULL pointer dereference exists in the function HuffmanDecoder::Get() located in huffmandecoder.hpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39516
pdftools_project -- pdftools	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function node::ObjNode::Value() located in objnode.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39538
pdftools_project -- pdftools	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Analyze::AnalyzeRoot() located in analyze.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39543

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pdftools_project -- pdftools	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Font::Size() located in font.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39542
pdftools_project -- pdftools	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function Analyze::AnalyzeXref() located in analyze.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39541
pdftools_project -- pdftools	An issue was discovered in pdftools through 20200714. A NULL pointer dereference exists in the function node::BDCNode::~BDCNode() located in bdcnode.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39539
pdftools_project -- pdftools	An issue was discovered in pdftools through 20200714. A stack-buffer-overflow exists in the function Analyze::AnalyzePages() located in analyze.cpp. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39540
sela_project -- sela	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function file::WavFile::WavFile() located in wav_file.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39549
sela_project -- sela	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.c has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39551
sela_project -- sela	An issue was discovered in sela through 20200412. file::WavFile::readFromFile() in wav_file.c has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39552
sela_project -- sela	An issue was discovered in sela through 20200412. file::SelaFile::readFromFile() in sela_file.cpp has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39550
sela_project -- sela	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function lpc::SampleGenerator::process() located in sample_generator.cpp. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39547
sela_project -- sela	An issue was discovered in sela through 20200412. file::WavFile::writeToFile() in wav_file.c has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39544
sela_project -- sela	An issue was discovered in sela through 20200412. rice::RiceDecoder::process() in rice_decoder.cpp has a heap-based buffer overflow.	2021-09-20	6.8	CVE-2021-39546
sela_project -- sela	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function rice::RiceDecoder::process() located in rice_decoder.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39545
sela_project -- sela	An issue was discovered in sela through 20200412. A NULL pointer dereference exists in the function frame::FrameDecoder::process() located in frame_decoder.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39548
swftools -- swftools	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function pool_read() located in pool.c. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39574
swftools -- swftools	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function main() located in swfdump.c. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39577
swftools -- swftools	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function string_hash() located in q.c. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39579
swftools -- swftools	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function swf_GetPlaceObject() located in swfobject.c. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39582

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
swftools -- swftools	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function rfx_alloc() located in mem.c. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39595
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function FileStream::makeSubStream() located in Stream.cc. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39562
swftools -- swftools	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function VectorGraphicOutputDev::drawGeneralImage() located in VectorGraphicOutputDev.cc. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39558
swftools -- swftools	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function OpAdvance() located in swfaction.c. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39569
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function grealloc() located in gmem.cc. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39553
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function Lexer::Lexer() located in Lexer.cc. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39554
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D0() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39555
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function InfoOutputDev::type3D1() located in InfoOutputDev.cc. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39556
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function copyString() located in gmem.cc. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39557
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function GString::~GString() located in GString.cc. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39559
swftools -- swftools	An issue was discovered in swftools through 20200710. A stack-buffer-overflow exists in the function Gfx::opSetFillColorN() located in Gfx.cc. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39561
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function dump_method() located in abc.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39575
swftools -- swftools	An issue was discovered in swftools through 20200710. A heap-buffer-overflow exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause code Execution.	2021-09-20	6.8	CVE-2021-39564
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_DumpActions() located in swfaction.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39563
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function params_dump() located in abc.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39590
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_GetShapeBoundingBox() located in swfshape.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39591

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_uint() located in pool.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39592
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_FontExtract_DefineFontInfo() located in swftext.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39593
swftools -- swftools	Other An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function updateusage() located in swftext.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39594
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_dump2() located in code.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39597
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function code_parse() located in code.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39596
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function parse_metadata() located in abc.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39589
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_ReadABC() located in abc.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39588
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function swf_DumpABC() located in abc.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39587
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function traits_dump() located in abc.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39585
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function namespace_set_hash() located in pool.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39584
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function pool_lookup_string2() located in pool.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39583
swftools -- swftools	An issue was discovered in swftools through 20200710. A NULL pointer dereference exists in the function callcode() located in code.c. It allows an attacker to cause Denial of Service.	2021-09-20	4.3	CVE-2021-39598
amazingweb -- wp-design-maps-places	The WP Design Maps & Places WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the filename parameter found in the ~/wpdmp-admin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.	2021-09-10	4.3	CVE-2021-38334
carrcommunications -- rsvpmaker_excel	The RSVPMaker Excel WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/phpexcel/PHPExcel/Shared/JAMA/docs/download.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.	2021-09-10	4.3	CVE-2021-38337
devondev -- simple_matted_thumbnails	The Simple Matted Thumbnails WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/simple-matted-thumbnail.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.01.	2021-09-10	4.3	CVE-2021-38339

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dj_emailpublish_project -- dj_emailpublish	The DJ EmailPublish WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/dj-email-publish.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.7.2.	2021-09-10	4.3	CVE-2021-38329
dreamfoxmedia -- woocommerce_payment_gateway_per_category	The WooCommerce Payment Gateway Per Category WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/includes/plugin_settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.10.	2021-09-10	4.3	CVE-2021-38341
elyazalee -- sms-ovh	The SMS OVH WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the position parameter found in the ~/sms-ovh-sent.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.1.	2021-09-10	4.3	CVE-2021-38357
feedify -- web_push_notifications	The Feedify – Web Push Notifications WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the feedify_msg parameter found in the ~/includes/base.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.1.8.	2021-09-10	4.3	CVE-2021-38352
notices_project -- notices	The Notices WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/notices.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.1.	2021-09-10	4.3	CVE-2021-38328
ops-robots-txt_project -- ops-robots-txt	The On Page SEO + Whatsapp Chat Button Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.	2021-09-10	4.3	CVE-2021-38332
outsidesource -- osd_subscribe	The OSD Subscribe WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the osd_subscribe_message parameter found in the ~/options/osd_subscribe_options_subscribers.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.3.	2021-09-10	4.3	CVE-2021-38351
spideranalyse_project -- spideranalyse	The spideranalyse WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the date parameter found in the ~/analyse/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.0.1.	2021-09-10	4.3	CVE-2021-38350
sw-guide -- edit_comments_xt	The Edit Comments XT WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/edit-comments-xt.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	2021-09-10	4.3	CVE-2021-38336
tromit -- yabp	The Yet Another bol.com Plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/yabp.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.	2021-09-10	4.3	CVE-2021-38330
ueberhamm-design -- youtube_video_inserter	The YouTube Video Inserter WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/adminUI/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.2.1.0.	2021-09-10	4.3	CVE-2021-38327
webodid -- dropdown_and_scrollable_text	The Dropdown and scrollable Text WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the content parameter found in the ~/index.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.	2021-09-10	4.3	CVE-2021-38353
wiseagent -- wise_agent_capture_forms	The Wise Agent Capture Forms WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/WiseAgentCaptureForm.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.	2021-09-10	4.3	CVE-2021-38335

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp_scrippets_project -- wp_scrippets	The WP Scrippets WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to a reflected $_SERVER["PHP_SELF"] value in the ~/wp-scrippets.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.5.1.	2021-09-10	4.3	CVE-2021-38333
wpleet -- post_title_counter	The Post Title Counter WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the notice parameter found in the ~/post-title-counter.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.	2021-09-10	4.3	CVE-2021-38326
zohocorp -- manageengine_desktop_central	Zoho ManageEngine DesktopCentral version 10.1.2119.7 and prior allows anyone to get a valid user's APIKEY without authentication.	2021-09-10	5	CVE-2021-37414
alipay_project -- alipay	A proid GET parameter of the WordPressæ”¯ä»˜å®?Alipay|è´¢ä»˜é€šTenpay|è´?å®?PayPalé›†æ?æ?’ä»¶ WordPress plugin through 3.7.2 is not sanitised, properly escaped or validated before inserting to a SQL statement not delimited by quotes, leading to SQL injection.	2021-09-06	6.5	CVE-2021-24390
arubanetworks -- arubaos	A remote path traversal vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.8.0.1, 8.7.1.4, 8.6.0.11, 8.5.0.13. Aruba has released patches for ArubaOS that address this security vulnerability.	2021-09-07	5.5	CVE-2021-37728
arubanetworks -- arubaos	A remote path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0-2.2.0.4; Prior to 8.7.1.3, 8.6.0.9, 8.5.0.12, 8.3.0.16, 6.5.4.19, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	5.5	CVE-2021-37729
arubanetworks -- sd-wan	A remote cross-site request forgery (csrf) vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.8.0.1, 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	2021-09-07	5.8	CVE-2021-37725
cashtomer_project -- cashtomer	An editid GET parameter of the Cashtomer WordPress plugin through 1.0.0 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	2021-09-06	6.5	CVE-2021-24391
cliniccases -- cliniccases	Multiple reflected cross-site scripting (XSS) vulnerabilities in ClinicCases 7.3.3 allow unauthenticated attackers to introduce arbitrary JavaScript by crafting a malicious URL. This can result in account takeover via session token theft.	2021-09-07	4.3	CVE-2021-38704
cliniccases -- cliniccases	messages_load.php in ClinicCases 7.3.3 suffers from a blind SQL injection vulnerability, which allows low-privileged attackers to execute arbitrary SQL commands through a vulnerable parameter.	2021-09-07	6.5	CVE-2021-38706
cliniccases -- cliniccases	ClinicCases 7.3.3 is affected by Cross-Site Request Forgery (CSRF). A successful attack would consist of an authenticated user following a malicious link, resulting in arbitrary actions being carried out with the privilege level of the targeted user. This can be exploited to create a secondary administrator account for the attacker.	2021-09-07	6.8	CVE-2021-38705
comment_highlighter_project -- comment_highlighter	A c GET parameter of the Comment Highlighter WordPress plugin through 0.13 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	2021-09-06	6.5	CVE-2021-24393
contiki-os -- contiki	In Contiki 3.0, Telnet option negotiation is mishandled. During negotiation between a server and a client, the server may fail to give the WILL/WONT or DO/DONT response for DO and WILL commands because of improper handling of exception condition, which leads to property violations and denial of service. Specifically, a	2021-09-05	5	CVE-2021-40523

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	server sometimes sends no response, because a fixed buffer space is available for all responses and that space may have been exhausted.			
cozyvision -- sms_alert_order_notifications	The SMS Alert Order Notifications WordPress plugin before 3.4.7 is affected by a cross site scripting (XSS) vulnerability in the plugin's setting page.	2021-09-06	4.3	CVE-2021-24588
easy_testimonial_manager_project -- easy_testimonial_manager	An id GET parameter of the Easy Testimonial Manager WordPress plugin through 1.2.0 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection	2021-09-06	6.5	CVE-2021-24394
eyoucms -- eyoucms	EyouCMS 1.5.4 is vulnerable to Open Redirect. An attacker can redirect a user to a malicious url via the Logout function.	2021-09-07	5.8	CVE-2021-39501
eyoucms -- eyoucms	A Cross-site scripting (XSS) vulnerability in Users in Qiong ICP EyouCMS 1.5.4 allows remote attackers to inject arbitrary web script or HTML via the `title` parameter in bind_email function.	2021-09-07	4.3	CVE-2021-39499
f-secure -- atlant	A vulnerability affecting F-Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine.	2021-09-07	4.3	CVE-2021-33599
file-upload-with-preview_project -- file-upload-with-preview	This affects the package file-upload-with-preview before 4.2.0. A file containing malicious JavaScript code in the name can be uploaded (a user needs to be tricked into uploading such a file).	2021-09-05	4.3	CVE-2021-23439
fortinet -- fortimanager	An improper access control vulnerability in FortiManager versions 6.4.0 to 6.4.3 may allow an authenticated attacker with a restricted user profile to access the SD-WAN Orchestrator panel via directly visiting its URL.	2021-09-06	6.5	CVE-2021-24006
fortinet -- fortisandbox	An improper access control vulnerability (CWE-284) in FortiSandbox versions 3.2.1 and below and 3.1.4 and below may allow an authenticated, unprivileged attacker to download the device configuration file via the recovery URL.	2021-09-06	4	CVE-2020-15939
gambit -- titan_framework	The iframe-font-preview.php file of the titan-framework does not properly escape the font-weight and font-family GET parameters before outputting them back in an href attribute, leading to Reflected Cross-Site Scripting issues	2021-09-06	4.3	CVE-2021-24435
geekwebsolution -- embed_youtube_video	The editid GET parameter of the Embed Youtube Video WordPress plugin through 1.0 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	2021-09-06	6.5	CVE-2021-24395
ghost -- ghost	Ghost is a Node.js content management system. An error in the implementation of the limits service between versions 4.0.0 and 4.9.4 allows all authenticated users (including contributors) to view admin-level API keys via the integrations API endpoint, leading to a privilege escalation vulnerability. This issue is patched in Ghost version 4.10.0. As a workaround, disable all non-Administrator accounts to prevent API access. It is highly recommended to regenerate all API keys after patching or applying the workaround.	2021-09-03	6.5	CVE-2021-39192
gibbonedu -- gibbon	A reflected XSS vulnerability exists in multiple pages in version 22 of the Gibbon application that allows for arbitrary execution of JavaScript (gibbonCourseClassID, gibbonPersonID, subpage, currentDate, or allStudents to index.php).	2021-09-03	4.3	CVE-2021-40492
gifsicle_project -- gifsicle	The find_color_or_error function in gifsicle 1.92 contains a NULL pointer dereference.	2021-09-07	5	CVE-2020-19752

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- inetutils	The ftp client in GNU Inetutils before 2.2 does not validate addresses returned by PASV/LSPV responses to make sure they match the server address. This is similar to CVE-2020-8284 for curl.	2021-09-03	4.3	CVE-2021-40491
google -- chrome	Heap buffer overflow in TabStrip in Google Chrome prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30614 FEDORA
google -- chrome	Use after free in Permissions in Google Chrome prior to 93.0.4577.63 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30607 FEDORA
google -- chrome	Use after free in Autofill in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30624 FEDORA
google -- chrome	Use after free in Bookmarks in Google Chrome prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30623 FEDORA
google -- chrome	Use after free in WebApp Installs in Google Chrome prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30622 FEDORA
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30620 FEDORA
google -- chrome	Inappropriate implementation in DevTools in Google Chrome prior to 93.0.4577.63 allowed a remote attacker who had convinced the user to use Chrome headless with remote debugging to execute arbitrary code via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30618 FEDORA
google -- chrome	Use after free in Media in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30616 FEDORA
google -- chrome	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30612 FEDORA
google -- chrome	Use after free in Sign-In in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30609 FEDORA
google -- chrome	Use after free in Blink in Google Chrome prior to 93.0.4577.63 allowed an attacker who convinced a user to drag and drop a malicous folder to a page to potentially perform a sandbox escape via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30606 FEDORA
google -- chrome	Use after free in Extensions API in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30610

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in Autofill in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to spoof security UI via a crafted HTML page.	2021-09-03	4.3	CVE-2021-30621 FEDORA
google -- chrome	Inappropriate implementation in Autofill in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to spoof security UI via a crafted HTML page.	2021-09-03	4.3	CVE-2021-30619 FEDORA
google -- chrome	Policy bypass in Blink in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to bypass site isolation via a crafted HTML page.	2021-09-03	4.3	CVE-2021-30617 FEDORA
google -- chrome	Inappropriate implementation in Navigation in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-09-03	4.3	CVE-2021-30615 FEDORA
google -- chrome	Use after free in Base internals in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30613 FEDORA
google -- chrome	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30611 FEDORA
google -- chrome	Use after free in Web Share in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-09-03	6.8	CVE-2021-30608 FEDORA
gpac -- gpac	An issue was discovered in gpac 0.8.0. The strdup function in box_code_base.c has a heap-based buffer over-read.	2021-09-07	5	CVE-2020-19750
gpac -- gpac	An issue was discovered in gpac 0.8.0. The gf_odf_del_ipmp_tool function in odf_code.c has a heap-based buffer over-read.	2021-09-07	6.4	CVE-2020-19751
jbl -- tune500bt_firmware	The Bluetooth Classic implementation on JBL TUNE500BT devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and shutdown a device by flooding the target device with LMP Feature Response data.	2021-09-07	6.1	CVE-2021-28155
jiangqie -- official_website_mini_program	The JiangQie Official Website Mini Program WordPress plugin before 1.1.1 does not escape or validate the id GET parameter before using it in SQL statements, leading to SQL injection issues	2021-09-06	6.5	CVE-2021-24303
linux -- linux_kernel	A race condition was discovered in ext4_write_inline_data_end in fs/ext4/inline.c in the ext4 subsystem in the Linux kernel through 5.13.13.	2021-09-03	4.4	CVE-2021-40490
moxa -- wac-2004_firmware	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP-323-JP-CT-T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	2021-09-07	4.3	CVE-2021-39278
mrdoc -- mrdoc	mrdoc is vulnerable to Deserialization of Untrusted Data	2021-09-06	6.8	CVE-2021-32568

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ntracker -- ntracker_usb_enterprise	A SQL-Injection vulnerability in the nTracker USB Enterprise(secure USB management solution) allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information.	2021-09-07	5	CVE-2020-7819
otrs -- otrs	It's possible to create an email which can be stuck while being processed by PostMaster filters, causing DoS. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions; 8.0.x version 8.0.15 and prior versions.	2021-09-06	5	CVE-2021-36093
otrs -- otrs	Malicious attacker is able to find out valid user logins by using the "lost password" feature. This issue affects: OTRS AG ((OTRS)) Community Edition version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions.	2021-09-06	5	CVE-2021-36095
parity -- frontier	Frontier is Substrate's Ethereum compatibility layer. Prior to commit number 0b962f218f0cdd796dadfe26c3f09e68f7861b26, a bug in `pallet-ethereum` can cause invalid transactions to be included in the Ethereum block state in `pallet-ethereum` due to not validating the input data size. Any invalid transactions included this way have no possibility to alter the internal Ethereum or Substrate state. The transaction will appear to have be included, but is of no effect as it is rejected by the EVM engine. The impact is further limited by Substrate extrinsic size constraints. A patch is available in commit number 0b962f218f0cdd796dadfe26c3f09e68f7861b26. There are no workarounds aside from applying the patch.	2021-09-03	5	CVE-2021-39193
phpwcms -- phpwcms	phpwcms v1.9 contains a cross-site scripting (XSS) vulnerability in /image_zoom.php.	2021-09-08	4.3	CVE-2020-19855
pureftpd -- pure-ftpd	In Pure-FTPd 1.0.49, an incorrect max_filesize quota mechanism in the server allows attackers to upload files of unbounded size, which may lead to denial of service or a server hang. This occurs because a certain greater-than-zero test does not anticipate an initial -1 value.	2021-09-05	5	CVE-2021-40524
python -- pillow	The package pillow from 0 and before 8.3.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the getrgb function.	2021-09-03	5	CVE-2021-23437
simplesystems -- libtiff	Buffer Overflow in LibTiff v4.0.10 allows attackers to cause a denial of service via the "invertImage()" function in the component "tiffcrop".	2021-09-07	5	CVE-2020-19131
swiftcrm -- club-management-software	An id GET parameter of the WordPress Membership SwiftCloud.io WordPress plugin through 1.0 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	2021-09-06	6.5	CVE-2021-24392
versa-networks -- versa_director	A XSS vulnerability exists in Versa Director Release: 16.1R2 Build: S8. An attacker can use the administration web interface URL to create a XSS based attack.	2021-09-07	4.3	CVE-2021-39285
vim -- vim	vim is vulnerable to Heap-based Buffer Overflow	2021-09-06	4.6	CVE-2021-3770 FEDORA
weechat -- weechat	WeeChat before 3.2.1 allows remote attackers to cause a denial of service (crash) via a crafted WebSocket frame that trigger an out-of-bounds read in plugins/relay/relay-websocket.c in the Relay plugin.	2021-09-05	5	CVE-2021-40516
wp-webhooks -- email_encoder	The Email Encoder â€“ Protect Email Addresses WordPress plugin before 2.1.2 has an endpoint that requires no authentication and will render a user supplied value in the HTML response without escaping or sanitizing the data.	2021-09-06	4.3	CVE-2021-24599
zmartzone -- mod_auth_openidc	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9.4, the 3rd-party init SSO functionality of mod_auth_openidc was reported to be vulnerable to	2021-09-03	5.8	CVE-2021-39191

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	an open redirect attack by supplying a crafted URL in the `target_link_uri` parameter. A patch in version 2.4.9.4 made it so that the `OIDCRedirectURLsAllowed` setting must be applied to the `target_link_uri` parameter. There are no known workarounds aside from upgrading to a patched version.			

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
addtoany -- addtoany_share_buttons	The AddToAny Share Buttons WordPress plugin before 1.7.46 does not sanitise its Sharing Header setting when outputting it in frontend pages, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-09-06	3.5	CVE-2021-24568
bluetrum -- ab5301a_firmware	The Bluetooth Classic implementation on Bluetrum AB5301A devices with unknown firmware versions does not properly handle the reception of oversized DM1 LMP packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.	2021-09-07	3.3	CVE-2021-34150
bookstackapp -- bookstack	bookstack is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-09-06	3.5	CVE-2021-3768
bookstackapp -- bookstack	bookstack is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-09-06	3.5	CVE-2021-3767
cliniccases -- cliniccases	Persistent cross-site scripting (XSS) vulnerabilities in ClinicCases 7.3.3 allow low-privileged attackers to introduce arbitrary JavaScript to account parameters. The XSS payloads will execute in the browser of any user who views the relevant content. This can result in account takeover via session token theft.	2021-09-07	3.5	CVE-2021-38707
dna88 -- highlight	The Highlight WordPress plugin before 0.9.3 does not sanitise its CustomCSS setting, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-09-06	3.5	CVE-2021-24591
espressif -- esp-idf	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly handle the reception of multiple LMP IO Capability Request packets during the pairing process, allowing attackers in radio range to trigger memory corruption (and consequently a crash) in ESP32 via a replayed (duplicated) LMP packet.	2021-09-07	3.3	CVE-2021-28136
eyoucms -- eyoucms	Eyoucms 1.5.4 lacks sanitization of input data, allowing an attacker to inject malicious code into `filename` param to trigger Reflected XSS.	2021-09-07	3.5	CVE-2021-39496
gdprinfo -- cookie_notice_\&_consent_banner_for_gdpr_\&_ccpa_compliance	The Cookie Notice & Consent Banner for GDPR & CCPA Compliance WordPress plugin before 1.7.2 does not properly sanitize inputs to prevent injection of arbitrary HTML within the plugin's design customization options.	2021-09-06	3.5	CVE-2021-24590
geminilabs -- site_reviews	The Site Reviews WordPress plugin before 5.13.1 does not sanitise some of its Review Details when adding a review as an admin, which could allow them to perform Cross-Site Scripting attacks when the unfiltered_html is disallowed	2021-09-06	3.5	CVE-2021-24603
jforum -- jforum	ViewCommon.java in JForum2 2.7.0 allows XSS via a user signature.	2021-09-04	3.5	CVE-2021-40509 FULLDISC
nextcloud -- circles	Nextcloud Circles is an open source social network built for the nextcloud ecosystem. In affected versions the Nextcloud Circles application is vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the Nextcloud Circles application is upgraded to 0.21.3, 0.20.10 or 0.19.14 to resolve this issue. As a workaround users may use a browser that has support for Content-Security-Policy. A notable exemption is Internet Explorer which does not support CSP properly.	2021-09-07	3.5	CVE-2021-32782

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
otrs -- otrs	It's possible to craft a request for appointment edit screen, which could lead to the XSS attack. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions.	2021-09-06	3.5	CVE-2021-36094
ti -- cc256xcqfn-em_firmware	The Bluetooth Classic implementation on the Texas Instruments CC256XCQFN-EM does not properly handle the reception of continuous LMP_AU_Rand packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after the paging procedure.	2021-09-07	3.3	CVE-2021-34149
trumani -- stop_spammers	The Stop Spammers Security | Block Spam Users, Comments, Forms WordPress plugin before 2021.18 does not escape some of its settings, allowing high privilege users such as admin to set Cross-Site Scripting payloads in them even when the unfiltered_html capability is disallowed	2021-09-06	3.5	CVE-2021-24517
web-settler -- form_builder	The Form Builder | Create Responsive Contact Forms WordPress plugin before 1.9.8.4 does not sanitise or escape its Form Title, allowing high privilege users such as admin to set Cross-Site Scripting payload in them, even when the unfiltered_html capability is disallowed	2021-09-06	3.5	CVE-2021-24513
wpfront -- wpfront_notification_bar	The WPFront Notification Bar WordPress plugin before 2.1.0.08087 does not properly sanitise and escape its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	2021-09-06	3.5	CVE-2021-24601
zh-jieli -- ac6901_firmware	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet.	2021-09-07	3.3	CVE-2021-31613
zh-jieli -- fw-ac63_bt_sdk	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.	2021-09-07	3.3	CVE-2021-34144