

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures (CVE) Report

16 - 31 Jan 2023

Vol. 10 No. 02

Table of Content				
Vendor	Product	Page Number		
Application				
	acrobat	1		
	acrobat_dc	8		
Adobe	acrobat_reader	21		
	acrobat_reader_dc	28		
	dimension	42		
amano	xoffice	42		
Apache	airflow	43		
nciipcdup	airflow_mysql_provider	43		
asynchttpclient_project	async-http-client	44		
ays-pro	survey_maker	48		
book_store_management _system_project	book_store_management_system	48		
builder	qwik	48		
Cakephp	cakephp	49		
	cx_cloud_agent	51		
	industrial_network_director	52		
	network_services_orchestrator	54		
Cisco	sip_ip_phone_software	59		
	telepresence_collaboration_endpoint	60		
	telepresence_tc	111		
	unified_communications_manager	114		
classroombookings	classroombookings	117		
contec	conprosys_hmi_system	117		
custom_404_pro_project	custom_404_pro	119		
daj	m-filter	120		
daloradius	daloradius	121		
Dell	cloud_mobility_for_dell_emc_storage	121		

Vendor	Product	Page Number
deno	deno	122
devolutions	remote_desktop_manager	123
e-dynamics	events_made_easy	124
ecommerce-codeigniter- bootstrap_project	ecommerce-codeigniter-bootstrap	125
Froxlor	froxlor	125
fullworksplugins	quick_event_manager	126
Glpi-project	glpi	127
gpac	gpac	129
healthchecks	healthchecks	130
html-stripscripts_project	html-stripscripts	130
	qradar_security_information_and_event_mana ger	131
IBM	robotic_process_automation	131
	robotic_process_automation_as_a_service	132
	robotic_process_automation_for_cloud_pak	133
inventory_system_projec t	inventory_system	134
jc21	nginx_proxy_manager	135
kalkun_project	kalkun	135
Keepass	keepass	136
libgit2	libgit2	136
lightftp_project	lightftp	138
login_with_phone_numb er_project	login_with_phone_number	138
matbao	wp_helper_premium	139
Mediawiki	mediawiki	139
Microsoft	edge_chromium	142
miniorange	ldap_integration_with_active_directory_and_o penldap	143
Misp	misp	143
Misp-project	malware_information_sharing_platform	144
modoboa	modoboa	144

Vendor	Product	Page Number	
my_youtube_channel_pro ject	my_youtube_channel	145	
Nlnetlabs	krill	147	
oi_yandex.maps_project	oi_yandex.maps	147	
online_food_ordering_sy stem_project	online_food_ordering_system	148	
online_tours_\&_travels_ management_system_pr oject	online_tours_\&_travels_management_system	148	
	access_manager	150 151 155 162 ge 163 L ^s 164 165	
	bi_publisher	151	
	business_intelligence	155	
	collaborative_planning	162	
	communications_billing_and_revenue_manage ment_elastic_charging_engine	163	
	communications_cloud_native_core_binding_s upport_function	164	
	communications_cloud_native_core_policy	165	
	communications_converged_application_serve r	166	
	communications_convergence	168	
Oracle	database	168	
	database_server	172	
	demantra_demand_management	174	
	e-business_suite	175	
	global_lifecycle_management_nextgen_oui_fra mework	177	
	graalvm	179	
	hcm_common_architecture	191	
	hospitality_reporting_and_analytics	191	
	isetup	194	
	isupplier_portal	195	
	jdk	195	
	jre	210	

Vendor	Product	Page Number
	learning_management	225
	marketing	226
	mobile_field_service	226
	mysql	227
	mysql_cluster	235
	mysql_server	238
	peoplesoft_enterprise_cs_academic_advisemen t	248
Oracle	peoplesoft_enterprise_peopletools	249
	primavera_gateway	252
	sales_for_handhelds	257
	sales_offline	258
	self-service_human_resources	259
	vm_virtualbox	260
	weblogic_server	269
	web_services_manager	281
orangescrum	orangescrum	282
pgadmin	pgadmin	282
Pimcore	pimcore	283
pkgconf	pkgconf	283
Plesk	obsidian	283
Powerdns	recursor	284
pyload	pyload	284
Rapid7	velociraptor	285
Redhat	openshift	288
rockstargames	grand_theft_auto_v	289
sandhillsdev	easy_digital_downloads	289
Shopware	shopware	290
signalwire	sofia-sip	293
strangerstudios	paid_memberships_pro	294
sudo_project	sudo	295
Tenable	nessus	296
theradsystem_project	theradsystem	297

Vendor	Product	Page Number
tpm2_software_stack_pr oject	tpm2_software_stack	298
trellix	skyhigh_secure_web_gateway	299
Trustwave	modsecurity	300
twinkletoessoftware	booked	301
unistra	impatient	301
VIM	vim	302
warfareplugins	social_warfare	302
Wireshark	wireshark	303
wp_topbar_project	wp_topbar	309
youtube_shortcode_proj ect	youtube_shortcode	309
zdir_project	zdir	310
Zohocorp	manageengine_exchange_reporter_plus	310
	manageengine_servicedesk_plus_msp	311
Hardware		
	maho-pbx_netdevancer	311
ate-mahoroba	maho-pbx_netdevancer_mobilegate	313
	maho-pbx_netdevancer_vsg	315
	email_security_appliance_c160	317
	email_security_appliance_c170	318
	email_security_appliance_c190	319
	email_security_appliance_c370	319
	email_security_appliance_c370d	320
	email_security_appliance_c380	321
Cisco	email_security_appliance_c390	322
	email_security_appliance_c670	322
	email_security_appliance_c680	323
	email_security_appliance_c690	324
	email_security_appliance_c690x	324
	email_security_appliance_x1070	325
	ip_phones_8832	326
	ip_phone_7800	327

Vendor	Product	Page Number
	ip_phone_7811	327
	ip_phone_7821	328
	ip_phone_7832	329
	ip_phone_7841	330
	ip_phone_7861	330
	ip_phone_8800	331
	ip_phone_8811	332
	ip_phone_8821	332
	ip_phone_8821-ex	333
	ip_phone_8831	334
	ip_phone_8832	334
	ip_phone_8841	335
	ip_phone_8845	336
	ip_phone_8851	337
	ip_phone_8861	337
Cisco	ip_phone_8865	338
CISCO	rv016	339
	rv042	340
	rv042g	342
	rv082	343
	rv160w_wireless-ac_vpn_router	345
	rv160_vpn_router	346
	rv260p_vpn_router_with_poe	347
	rv260_vpn_router	347
	rv340	348
	rv340w	349
	rv345	351
	rv345p	352
	unified_ip_phone_8851nr	353
	unified_ip_phone_8865nr	353
	webex_room_phone	354
	webex_share	355

Vendor	Product	Page Number	
Cisco	wireless_ip_phone_8821	356	
CISCO	wireless_ip_phone_8821-ex	357	
	powervault_me5012	358	
Dell	powervault_me5024	358	
	powervault_me5084	358	
Omnon	cp1l-el20dr-d	359	
Omron	cx-motion-mch	360	
pixela	pix-rt100	360	
Sonicwall	sma1000	361	
Tenda	ac18	361	
Tp-link	tl-sg105pe	362	
Trendnet	tew-820ap	363	
Operating System			
Apple	macos	366	
	maho-pbx_netdevancer_firmware	373	
ate-mahoroba	maho-pbx_netdevancer_mobilegate_firmware	375	
	maho-pbx_netdevancer_vsg_firmware	377	
	asyncos	379	
	ip_phones_8832_firmware	380	
	ip_phone_7800_firmware	380	
	ip_phone_7811_firmware	381	
	ip_phone_7821_firmware	382	
	ip_phone_7832_firmware	383	
	ip_phone_7841_firmware	383	
Cisco	ip_phone_7861_firmware	384	
	ip_phone_8800_firmware	385	
	ip_phone_8811_firmware	385	
	ip_phone_8821-ex_firmware	386	
	ip_phone_8821_firmware	387	
	ip_phone_8831_firmware	388	
	ip_phone_8832_firmware	388	
	ip_phone_8841_firmware	389	

Vendor	Product	Page Number
	ip_phone_8845_firmware	390
	ip_phone_8851_firmware	390
	ip_phone_8861_firmware	391
	ip_phone_8865_firmware	392
	roomos	393
	rv016_firmware	401
	rv042g_firmware	403
	rv042_firmware	404
	rv082_firmware	406
	rv160w_wireless-ac_vpn_router_firmware	407
	rv160_vpn_router_firmware	408
Cisco	rv260p_vpn_router_with_poe_firmware	409
	rv260_vpn_router_firmware	410
	rv340w_firmware	411
	rv340_firmware	412
	rv345p_firmware	413
	rv345_firmware	414
	unified_ip_phone_8851nr_firmware	415
	unified_ip_phone_8865nr_firmware	416
	webex_room_phone_firmware	416
	webex_share_firmware	417
	wireless_ip_phone_8821-ex_firmware	418
	wireless_ip_phone_8821_firmware	419
Debian	debian_linux	420
	powervault_me5012_firmware	422
Dell	powervault_me5024_firmware	422
	powervault_me5084_firmware	423
Fedoraproject	fedora	423
Google	android	424
Linux	linux_kernel	441
Microsoft	windows	444
Omron	cp1l-el20dr-d_firmware	452

Vendor	Product	Page Number
Omron	cx-motion-mch_firmware	453
Oracle	solaris	453
pixela	pix-rt100_firmware	456
Redhat	openshift	457
Sonicwall	sma1000_firmware	458
Tenda	ac18_firmware	459
Tp-link	tl-sg105pe_firmware	460
Trendnet	tew-820ap_firmware	460
zephyrproject	zephyr	463

Common Vulnerabilities and Exposures (CVE) Report					
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Application		
Vendor: Ad	obe				
Product: ac	robat				
Affected Ver	sion(s): From (i	ncluding)	20.001.30005 Up to (inclu	iding) 20.005.304	418
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/1
Stack- based Buffer Overflow	18-Jan-2023	7.8	21579 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/2

0-1

1-2

2-3

3-4 4-5 Page **1** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. CVE ID : CVE-2023-		
			21604		
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21605	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/3
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/4

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21606		
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21607	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/5
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21608	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/6

0-1

1-2

2-3

3-4 4-5 Page **3** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/7
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21610	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/8
Exposure of Resource	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx. adobe.com/se curity/produc	A-ADO- ACRO- 020223/9

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21611	ts/acrobat/ap sb23-01.html	
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21612	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/10

0-1

1-2

2-3

3-4 4-5 Page **5** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21581	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/11
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21585	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/12

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21613	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/13
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21614	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/14

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: act	Product: acrobat_dc								
Affected Ver	sion(s): From (i	ncluding)	15.008.20082 Up to (inclu	ıding) 22.003.202	281				
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21579	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/15				
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21604	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/16				

0-1

1-2

2-3

3-4 4-5 Page **8** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21605	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/17
Out-of- bounds Write	18-Jan-2023	7.8	21605 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21606	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/18
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx. adobe.com/se curity/produc	A-ADO- ACRO- 020223/19

0-1

1-2

2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	ts/acrobat/ap sb23-01.html	
Use After Free	18-Jan-2023	7.8	21607 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/20
Out-of- bounds Write	18-Jan-2023	7.8	CVE ID : CVE-2023- 21608 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/21

0-1

1-2

2-3

3-4 4-5 Page **10** of **463** 8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609		
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21610	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/22
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/23

0-1

1-2

2-3

3-4 4-5 Page **11** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21611		
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21612	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/24
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/25

0-1

1-2

2-3

3-4 4-5 Page **12** of **463** 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21581		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21585	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/26
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/27

0-1

1-2

2-3

3-4 4-5 Page **13** of **463** 6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21613		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21614	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/28
Affected Ver	sion(s): From (i	ncluding)	15.008.20082 Up to (inclu	iding) 22.003.202	282
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/29

0-1

1-2

2-3

3-4 4-5 Page **14** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21579		
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21604	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/30
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/31

0-1

1-2

2-3

3-4 4-5 Page **15** of **463** 5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21605		
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21606	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/32
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/33

0-1

1-2

2-3

3-4 4-5 Page **16** of **463** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. CVE ID : CVE-2023-		
			21607		
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21608	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/34
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/35

0-1

1-2

2-3

3-4 4-5 Page **17** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21610	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/36
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21611	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/37

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21612	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/38
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21581	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/39

0-1

1-2

2-3

3-4 4-5 Page **19** of **463** 5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21585	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/40
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21613	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/41

0-1

1-2

2-3

3-44-5Page 20 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21614	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/42
	robat_reader				
Affected Ver	sion(s): From (i	ncluding)	20.001.30005 Up to (inclu	iding) 20.005.304	418
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/43

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21579		
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21604	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/44
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21605	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/45

0-1

1-2

2-3

3-4 4-5 Page **22** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21606	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/46
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21607	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/47
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx. adobe.com/se curity/produc	A-ADO- ACRO- 020223/48

0-1

1-2

2-3

3-4 4-5 Page **23** of **463** 6-7 7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	ts/acrobat/ap sb23-01.html	
Out-of- bounds Write	18-Jan-2023	7.8	21608 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/49
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/50

0-1

1-2

2-3

3-4 4-5 Page **24** of **463**

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21610		
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21611	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/51
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/52

0-1

1-2

2-3

3-4 4-5 Page **25** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21612		
Out-of- bounds Read	18-Jan-2023	5.5	21612 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21581	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/53
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/54

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21585		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21613	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/55
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/56

0-1

1-2

2-3

3-4 4-5 Page **27** of **463** 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-		
Product: ac	robat_reader_c		21614		
			15.008.20082 Up to (inclu	uding) 22 003 20	281
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21579	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/57
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/58

0-1

1-2

2-3

3-4 4-5 Page **28** of **463** 5-6

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21604		
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21605	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/59
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/60

0-1

1-2

2-3

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21606		
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21607	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/61
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/62

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file.		
			CVE ID : CVE-2023- 21608		
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/63
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/64

0-1

1-2

2-3

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21610		
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21611	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/65
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/66

0-1

1-2

2-3

3-4 4-5 Page **32** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. CVE ID : CVE-2023- 21612		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21581	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/67
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/68

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. CVE ID : CVE-2023- 21585		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21613	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/69
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/70

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file.		
			CVE ID : CVE-2023- 21614		
Affected Ver	sion(s): From (i	ncluding)	15.008.20082 Up to (inclu	iding) 22.003.202	282
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/71
			21579		
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/72

0-1

1-2

2-3

3-4 4-5 Page **35** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file.		
			CVE ID : CVE-2023- 21604		
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21605	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/73
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/74

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21606		
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21607	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/75
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21608	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/76

0-1

1-2

2-3

3-4 4-5 Page **37** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/77
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21610	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/78
Exposure of Resource	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx. adobe.com/se curity/produc	A-ADO- ACRO- 020223/79

0-1

1-2

2-3

3-4 4-5 Page **38** of **463**

5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21611	ts/acrobat/ap sb23-01.html	
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21612	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/80

0-1

1-2

2-3

3-4 4-5 Page **39** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21581	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/81
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21585	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/82

0-1

1-2

2-3

3-4 4-5 Page **40** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21613	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/83
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21614	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	A-ADO- ACRO- 020223/84

0-1

1-2

2-3

3-4 4-5 Page **41** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: dimension									
Affected Vers	Affected Version(s): * Up to (including) 3.4.6								
Use After Free	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21601	https://helpx. adobe.com/se curity/produc ts/dimension /apsb23- 10.html	A-ADO- DIME- 020223/85				
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21603	https://helpx. adobe.com/se curity/produc ts/dimension /apsb23- 10.html	A-ADO- DIME- 020223/86				
Vendor: amano									
Product: xoffice									
Affected Vers	sion(s): 7.1.387	9							

0-1

1-2

2-3

3-4 4-5 Page **42** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	24-Jan-2023	9.8	Amano Xoffice parking solutions 7.1.3879 is vulnerable to SQL Injection. CVE ID : CVE-2023- 23331	N/A	A-AMA- XOFF- 020223/87
Vendor: Apa	ache			L	
Product: air	flow				
Affected Ver	sion(s): * Up to	(excluding	g) 2.5.1		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	21-Jan-2023	9.8	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow, Apache Software Foundation Apache Airflow MySQL Provider.This issue affects Apache Airflow: before 2.5.1; Apache Airflow MySQL Provider: before 4.0.0. CVE ID : CVE-2023- 22884	https://githu b.com/apache /airflow/pull/ 28811	A-APA-AIRF- 020223/88
Product: air	flow_mysql_pi	rovider		•	
Affected Ver	sion(s): * Up to	(excludin	g) 4.0.0		
Improper Neutralizat ion of Special Elements used in a Command ('Comman	21-Jan-2023	9.8	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow, Apache Software Foundation	https://githu b.com/apache /airflow/pull/ 28811	A-APA-AIRF- 020223/89

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			Apache Airflow MySQL Provider.This issue affects Apache Airflow: before 2.5.1; Apache Airflow MySQL Provider: before 4.0.0.		
			CVE ID : CVE-2023- 22884		
Vendor: asy	/nchttpclient_p	roject			
Product: as	ync-http-client	;			
Affected Ver	sion(s): * Up to	(excluding	g) 1.4.1		
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was	N/A	A-ASY-ASYN- 020223/90

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended. In general, this is unlikely to result in data disclosure, but it can result in a number of logical errors and other misbehaviours.		
			CVE ID : CVE-2023- 0040		
Affected Ver	sion(s): From (i	ncluding)	1.10.0 Up to (excluding) 1	.12.1	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was intended. In general, this is unlikely to result in data disclosure, but it	N/A	A-ASY-ASYN- 020223/91

0-1

1-2

2-3

3-4 4-5 Page **45** of **463** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			can result in a number of logical errors and other misbehaviours. CVE ID : CVE-2023- 0040						
Affected Ver	Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.13.2								
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was intended. In general, this is unlikely to result in data disclosure, but it can result in a number of logical errors and other misbehaviours.	N/A	A-ASY-ASYN- 020223/92				

0-1

1-2

2-3

3-4 4-5 Page **46** of **463** 6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0040		
Affected Ver	sion(s): From (i	ncluding)	1.5.0 Up to (excluding) 1.9	0.1	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was intended. In general, this is unlikely to result in data disclosure, but it can result in a number of logical errors and other misbehaviours. CVE ID : CVE-2023- 0040	N/A	A-ASY-ASYN- 020223/93

0-1

1-2

2-3

3-4 4-5 Page **47** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Vendor: ays	s-pro	<u> </u>				
Product: su	rvey_maker					
Affected Ver	sion(s): * Up to	(excluding	g) 3.1.2			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-2023	8.8	The Survey Maker WordPress Plugin, version < 3.1.2, is affected by an authenticated SQL injection vulnerability in the 'surveys_ids' parameter of its 'ays_surveys_export_jso n' action. CVE ID : CVE-2023- 23490	N/A	A-AYS-SURV- 020223/94	
Vendor: boo	ok store mana	gement s	system_project			
	ok_store_mana	<u> </u>	· · ·			
Affected Ver		-				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	Book Store Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in /bsms_ci/index.php/bo ok. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the writer parameter. CVE ID : CVE-2023- 23024	N/A	A-BOO- BOOK- 020223/95	
Vendor: bui				·		
Product: qw						
Affected Version(s): * Up to (excluding) 0.16.2						
Affected Ver	1			i i	A-BUI-QWIK-	

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			GitHub repository builderio/qwik prior to 0.1.0-beta5. CVE ID : CVE-2023- 0410	/2da583f0- 7f66-4ba7- 9bed- 8e7229aa578 e, https://githu b.com/builder io/qwik/com mit/4b2f89db bd2bc0a2c92 eae1a49bdd1 86e589151a	
Vendor: Cal	kephp				
Product: ca	kephp				
Affected Ver	sion(s): From (i	ncluding)	4.2.0 Up to (excluding) 4.2	2.12	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2023	9.8	CakePHP is a development framework for PHP web apps. In affected versions the `Cake\Database\Query: :limit()` and `Cake\Database\Query: :offset()` methods are vulnerable to SQL injection if passed un- sanitized user request data. This issue has been fixed in 4.2.12, 4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue. CVE ID : CVE-2023- 22727	https://baker y.cakephp.org /2023/01/06 /cakephp_421 1_4311_4410_ released.html, https://githu b.com/cakeph p/cakephp/co mmit/3f463e 7084b5a15e6 7205ced3a62 2577cca7a23 9	A-CAK-CAKE- 020223/97

0-1

1-2

2-3

3-4 4-5 Page **49** of **463** 6-7 7-8

5-6

Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.11 Improper Neutralization of Special Elements 17-Jan-2023 9.8 17-Jan-2023 9.8 18-Elements 19.8 19.8 19.8 17-Jan-2023 9.8 17-Jan-2023 9.8 17-Jan-2023 9.8 17-Jan-2023 9.8 18-Elements 19.6 19.7 100 of Special Elements 19.8 101 of Special Injection ') 102 of Special Injection ') 103 of Special Injection ') 104 of Special Injection ') 105 of Special Elements Improper Neutralization of Special Improper Neutralization of Special Improper Neutralization of Special Ilements Ingection ') 17-	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Improper Neutralizat ion of Special Elements (SQL Injection')17-Jan-20239.8development framework for PHP web apps. In affected versions the 'Cake\Database\Query: :limit()`and 'Cake\Database\Query: injection if passed un- sanitized user request data. This issue has been fixed in 4.2.12,https://baker y.cakeph.org /2023/01/06 /cakephp.421 1.4311.4410, released.html, https://githu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu btms:/jgithu 	Affected Ver	Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.11							
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')Interest of the second s	Neutralizat ion of Special Elements used in an SQL Command ('SQL	17-Jan-2023	9.8	development framework for PHP web apps. In affected versions the `Cake\Database\Query: :limit()` and `Cake\Database\Query: :offset()` methods are vulnerable to SQL injection if passed un- sanitized user request data. This issue has been fixed in 4.2.12, 4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue. CVE ID : CVE-2023-	y.cakephp.org /2023/01/06 /cakephp_421 1_4311_4410_ released.html, https://githu b.com/cakeph p/cakephp/co mmit/3f463e 7084b5a15e6 7205ced3a62 2577cca7a23				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')17-Jan-20239.8development framework for PHP web apps. In affected 'Cake\Database\Query: 1_4311_4410_ released.html, b.com/cakeph b.com/cakephA-CAK-CAKE- 020223/99SQL Command ('SQL Injection')9.817-Jan-20239.8A-CAK-CAKE- 020223/99	Affected ver	sion(s): From (i	ncluaing		F.10				
CVSS Scoring Scale 0-1 1-2 _2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Neutralizat ion of Special Elements used in an SQL Command ('SQL	17-Jan-2023	9.8	development framework for PHP web apps. In affected versions the `Cake\Database\Query: :limit()` and `Cake\Database\Query: :offset()` methods are vulnerable to SQL injection if passed un- sanitized user request data. This issue has	y.cakephp.org /2023/01/06 /cakephp_421 1_4311_4410_ released.html, https://githu b.com/cakeph p/cakephp/co mmit/3f463e 7084b5a15e6				
	CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue. CVE ID : CVE-2023-	2577cca7a23 9	
Vendor: Cis			22727		
	_cloud_agent				
	sion(s): * Up to	(excluding	g) 1.9		
Incorrect Default Permission s	20-Jan-2023	6.7	A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to insecure file permissions. An attacker could exploit this vulnerability by calling the script with sudo. A successful exploit could allow the attacker to take complete control of the affected device. CVE ID : CVE-2023- 20043	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- cxagent- gOq9QjqZ	A-CIS-CX_C- 020223/100
Affected Ver	<mark>sion(s): * Up to</mark> 20-Jan-2023	(excluding	g) 2.2.1 A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci	A-CIS-CX_C- 020223/101

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insecure file permissions. An attacker could exploit this vulnerability by persuading support to update settings which call the insecure script. A successful exploit could allow the attacker to take complete control of the affected device. CVE ID : CVE-2023- 20044	sco-sa- cxagent- gOq9QjqZ	
Affected Vers	sion(s): 2.2				
Incorrect Default Permission s	20-Jan-2023	6.7	A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to insecure file permissions. An attacker could exploit this vulnerability by calling the script with sudo. A successful exploit could allow the attacker to take complete control of the affected device. CVE ID : CVE-2023- 20043	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- cxagent- gOq9QjqZ	A-CIS-CX_C- 020223/102
Product: inc	lustrial_netwo	rk_direct	cor		
Affected Vers	sion(s): * Up to	(excluding	g) 1.6.0		
Use of Hard- coded Credentials	20-Jan-2023	8.8	A vulnerability in the monitoring application of Cisco Industrial Network Director could allow an authenticated, local attacker to access a static secret key used	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci	A-CIS-INDU- 020223/103
CVSS Scoring S	icale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 52 of 463	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to store both local data and credentials for accessing remote systems. This vulnerability is due to a static key value stored in the application used to encrypt application data and remote credentials. An attacker could exploit this vulnerability by gaining local access to the server Cisco Industrial Network Director is installed on. A successful exploit could allow the attacker to decrypt data allowing the attacker to access remote systems monitored by Cisco Industrial Network Director. CVE ID : CVE-2023- 20038	sco-sa-ind- fZyVjJtG	
Affected Ver	sion(s): * Up to	(excluding	g) 1.7.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	5.4	A vulnerability in Cisco Industrial Network Director could allow an authenticated, remote attacker to conduct stored cross-site scripting (XSS) attacks. The vulnerability is due to improper validation of content submitted to the affected application. An attacker could exploit this vulnerability by sending requests containing malicious	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ind- fZyVjJtG	A-CIS-INDU- 020223/104

0-1

1-2

2-3

3-4 4-5 Page **53** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values to the affected system. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. CVE ID : CVE-2023-		
D			20037		
	twork_service	s_orchest	rator		
Affected Ver			A vulnerability in the		
Unrestricte d Upload of File with Dangerous Type	20-Jan-2023	5.5	NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-nso- path-trvsl- zjBeMkZg	A-CIS-NETW- 020223/105

0-1

1-2

2-3

3-4 4-5 Page **54** of **463** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless therun-as-user option is used. CVE ID : CVE-2023- 20040		
Affected Ver	sion(s): From (i	ncluding)	3.3 Up to (excluding) 5.4.7		
Unrestricte d Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-nso- path-trvsl- zjBeMkZg	A-CIS-NETW- 020223/106

0-1

1-2

2-3

3-4 4-5 Page **55** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless therun-as-user option is used. CVE ID : CVE-2023- 20040		
Affected Ver	sion(s): From (i	ncluding)	5.5 Up to (excluding) 5.5.6		
Unrestricte d Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-nso- path-trvsl- zjBeMkZg	A-CIS-NETW- 020223/107

0-1

1-2

2-3

3-4 4-5 Page **56** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless therun-as-user option is used. CVE ID : CVE-2023- 20040		
Affected Ver	sion(s): From (i	ncluding)	5.6 Up to (excluding) 5.6.7	7	
Unrestricte d Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-nso- path-trvsl- zjBeMkZg	A-CIS-NETW- 020223/108

0-1

1-2

2-3

3-4 4-5 Page **57** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless therun-as-user option is used. CVE ID : CVE-2023- 20040		
Affected Ver	sion(s): From (i	ncluding)	5.7 Up to (excluding) 5.7.4		
Unrestricte d Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-nso- path-trvsl- zjBeMkZg	A-CIS-NETW- 020223/109

0-1

1-2

2-3

3-4 4-5 Page **58** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless therun-as-user option is used. CVE ID : CVE-2023- 20040		
Product: sin	p_ip_phone_sof	tware	20040		
	sion(s): * Up to		y) 1.2.0		
Allocation of Resources Without Limits or Throttling	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-lldp- memlk- McOecPT	A-CIS-SIP 020223/110

0-1

1-2

2-3

3-4 4-5 Page **59** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.		
			CVE ID : CVE-2023- 20047		
Product: tel	lepresence_col	laboratio	n_endpoint		
Affected Ver	sion(s): 8.0.0				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/111
Affected Ver	sion(s): 8.0.1		20008		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 60 of 463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/112
Affected Ver	sion(s): 8.1.0		20008		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/113

0-1

1-2

2-3

3-4 4-5 Page **61** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Affected Ver	sion(s): 8.1.1				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/114
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-TELE- 020223/115

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
Affected Ver	sion(s): 8.2.0				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/116

0-1

1-2

2-3

3-4 4-5 Page **63** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrite arbitrary files on the affected device. CVE ID : CVE-2023-		
			20008		
Affected Ver	sion(s): 8.2.1				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/117
Affected Ver	sion(s): 8.2.2		-	-	
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/118

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
Affected Ver	cion(a): 0.2.0		CVE ID : CVE-2023- 20008		
Anected ver	sion(s): 8.3.0		A vulnerability in the		
N/A	20-Jan-2023	7.1	CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/119

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/120
Affected Ver	sion(s): 8.3.1				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/121

0-1

1-2

2-3

3-4 4-5 Page **66** of **463** 6-7

5-6

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023-		
			20008		
Affected Ver	sion(s): 8.3.2				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/122
Allected ver	sion(s): 8.3.3		A vulnerability in the	https://sec.cl	
N/A	20-Jan-2023	7.1	CLI of Cisco TelePresence CE and	oudapps.cisco .com/security	A-CIS-TELE- 020223/123
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 67 of 463	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	/center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
			20008		
Affected Ver	sion(s): 8.3.5		A such such i lites in the		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/124

0-1

1-2

2-3

3-4 4-5 Page **68** of **463** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/125
Affected Ver	sion(s): 8.3.6				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/126

0-1

1-2

2-3

3-4 4-5 Page **69** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023-		
Affected Ver	sion(s): 9.0.1		20008		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/127

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/128
Affected Ver	sion(s): 9.1.1				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/129

0-1

1-2

2-3

3-4 4-5 Page **71** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/130
Affected Ver	sion(s): 9.1.2			<u> </u>	
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-TELE- 020223/131

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/132

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sourced from the affected system. CVE ID : CVE-2023-		
			20002		
Affected Ver	sion(s): 9.1.3				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/133
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/134

0-1

1-2

2-3

3-4 4-5 Page **74** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.1.4				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/135

0-1

1-2

2-3

3-4 4-5 Page **75** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/136
Affected Ver	sion(s): 9.1.5				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/137

0-1

1-2

2-3

3-4 4-5 Page **76** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/138
Affected Ver	sion(s): 9.1.6				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-	A-CIS-TELE- 020223/139

0-1

1-2

2-3

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/140

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.10.1			L	
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/141
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/142

0-1

1-2

2-3

3-4 4-5 Page **79** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.		
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.10.2				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/143
Server- Side Request	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-TELE- 020223/144

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023-	nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
			20002		
Affected Ver	sion(s): 9.10.3				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/145

0-1

1-2

2-3

3-4 4-5 Page **81** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/146
Affected Ver	sion(s): 9.12.3				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/147

0-1

1-2

2-3

3-4 4-5 Page **82** of **463** 5-6

6-7

8-9

Side Request Forgery20-Jan-20234.4user-supplied input. An attacker could exploit this vulnerability by/center/conte nt/CiscoSecur ityAdvisory/ciA-CIS-TELE- 020223/148	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server- Side Request Forgery (SSRF)20-Jan-20234.4TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network request that are sourced from the affected system.https://sec.cl oudaps.cisco .com/security /center/conter ht/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRKA-CIS-TELE- 020223/148				are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
Affected Version(s): 9124	Server- Side Request Forgery (SSRF)		4.4	TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023-	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos-	
	Affected Ver	sion(s): 9.12.4				

0-1

1-2

2-3

3-4 4-5 Page **83** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/149
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/150

0-1

1-2

2-3

3-4 4-5 Page **84** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.		
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.12.5				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/151
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-	A-CIS-TELE- 020223/152

0-1

1-2

2-3

3-4 4-5 Page **85** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023-	roomos- dkjGFgRK	
Affected Ver	sion(s): 9.13.0		20002		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/153

0-1

1-2

2-3

3-4 4-5 Page **86** of **463** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/154
Affected Ver	sion(s): 9.13.1		<u> </u>		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/155

0-1

1-2

2-3

3-4 4-5 Page **87** of **463** 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/156
Affected Ver	sion(s): 9.13.2				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-TELE- 020223/157

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/158

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sourced from the affected system. CVE ID : CVE-2023-		
			20002		
Affected Ver	sion(s): 9.13.3			r	
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/159
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/160

0-1

1-2

2-3

3-4 4-5 Page **90** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.14.3		1		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/161

0-1

1-2

2-3

3-4 4-5 Page **91** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/162
Affected Ver	sion(s): 9.14.4				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/163

0-1

1-2

2-3

3-4 4-5 Page **92** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/164
Affected Ver	sion(s): 9.14.5			L	
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-	A-CIS-TELE- 020223/165

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/166

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.14.6			I	
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/167
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/168

0-1

1-2

2-3

3-4 4-5 Page **95** of **463** 6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.		
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.15.0.1	.0			
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/169
Server- Side Request	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cl oudapps.cisco .com/security /center/conte	A-CIS-TELE- 020223/170

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.15.0.1	.1			
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/171

0-1

1-2

2-3

3-4 4-5 Page **97** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/172
Affected Ver	sion(s): 9.15.10	8			
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/173

0-1

1-2

2-3

3-4 4-5 Page **98** of **463** 5-6

6-7

7-8

Server- Side Request Forgery (SSRF)20-Jan-20234.4A a controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.Https://sec.cl oudaps.cisco .com/security /center/content through an affected device. This vulnerability is due to improper validation of through an affected device to a user of the web application. A successful exploit could allow the attacker to sending a crafted request to a user of the web application. A successful exploit could allow the attacker to sending a crafted request that are sourced from the affected system. CVE ID : CVE-2023- 20002Https://sec.cl oudaps.cisco .com/security /center/content th/ciscoSecurity digGFgRKA-CIS-TELE- 02023/174Affected Version(s): 9.15.13.09.1000000000000000000000000000000000000	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server- Side Request Forgery (SSRF)20-Jan-20234.4TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. Thishttps://sec.cl oudaps.cisco .com/security /center/conter https://sec.cl oudaps.cisco .com/security (SSRF)A-CIS-TELE- 020223/174Server- Side Request Forgery (SSRF)20-Jan-20234.4A-MA-CIS-TELE- 020223/174A-CIS-TELE- 020223/174CVE ID : CVE-2023- 20002CVE ID : CVE-2023- 20002Sco-sa- roomos- dkjGFgRKA-CIS-TELE- 020223/174				are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023-		
	Side Request Forgery (SSRF)			A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023-	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos-	

0-1

1-2

2-3

3-4 4-5 Page **99** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/175
Affected Ver	sion(s): 9.15.3.2	25	20000		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/176

0-1

1-2

2-3

3-4 4-5 Page **100** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/177
Affected Ver	<mark>sion(s): 9.15.3.2</mark>	26		1	1
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci	A-CIS-TELE- 020223/178

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	sco-sa- roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/179

0-1

1-2

2-3

3-4 4-5 Page **102** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 20002					
Affected Version(s): 9.15.8.12								
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/180			
Affected Ver	sion(s): 9.2.1							
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/181			

0-1

1-2

2-33-44-5Page 103 of 463

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/182
Affected Ver	sion(s): 9.2.2			·	
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco	https://sec.cl oudapps.cisco	A-CIS-TELE- 020223/183
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 <u>9</u> -10

Page 104 of 463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	.com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/184

0-1

1-2

2-33-44-5Page 105 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send arbitrary network requests that are sourced from the affected system.		
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 9.2.3				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/185
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/186

0-1

1-2

 2-3
 3-4
 4-5

 Page 106 of 463

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.		
Affected Ver	sion(s): 9.2.4		CVE ID : CVE-2023- 20002		
			A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated,		
N/A	20-Jan-2023	7.1	local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/187

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/188
Affected Ver	sion(s): 9.9.3				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/189

0-1

1-2

2-3

3-4 4-5 Page **108** of **463** 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023 -		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	20008 A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/190
Affected Ver	sion(s): 9.9.4				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-TELE- 020223/191

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/192

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Descri	ption & CVI	E ID	Pat	ch	NCI	PC ID	
			sourced from the affected system. CVE ID : CVE-2023- 20002							
Product: telepresence_tc										
Affected Ver	sion(s): 7.3.13									
N/A	20-Jan-2023	7.1	improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a		https:// oudapps .com/se /center, nt/Cisco ityAdvis sco-sa- roomos- dkjGFgF	s.cisco curity /conte oSecur sory/ci	A-CIS- 02022	TELE- 3/193		
Affected Ver	sion(s): 7.3.21			1	1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This		https:// oudapps .com/se /center, nt/Cisco ityAdvis sco-sa-	s.cisco curity /conte oSecur	A-CIS- 02022	TELE- 3/194		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	
CADD PROFILING 2		12 2		4-5	5-0	0-7	7-0	6-5	010	

Page **111** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	roomos- dkjGFgRK	
			20008		
Affected Ver	sion(s): 7.3.5				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/195

0-1

1-2

2-3

3-4 4-5 Page **112** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20008		
Affected Ver	sion(s): 7.3.6				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/196
Affected Ver	sion(s): 7.3.7				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/197

0-1

1-2

2-3 3-4 4-5 Page **113** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Affected Ver	sion(s): 7.3.9				
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	A-CIS-TELE- 020223/198
Product: un	ified_commun	ications_	nanager		
		_			

0-1

1-2

2-33-44-5Page 114 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): * Up to (excluding) 12.5\\(1\\)su7							
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-2023	8.8	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low- privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges. CVE ID : CVE-2023- 20010	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-cucm- sql-rpPczR8n	A-CIS-UNIF- 020223/199		
Affected Ver	sion(s): From (i	ncluding)	11.5\\(1\\) Up to (exclud	1	su7		
Improper Neutralizat ion of Special Elements	20-Jan-2023	8.8	A vulnerability in the web-based management interface of Cisco Unified Communications	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	A-CIS-UNIF- 020223/200		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Page **115** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low- privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges. CVE ID : CVE-2023- 20010	ityAdvisory/ci sco-sa-cucm- sql-rpPczR8n	
Affected Ver	sion(s): From (i	ncluding)	14.0 Up to (excluding) 14s	su2	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-2023	8.8	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-cucm- sql-rpPczR8n	A-CIS-UNIF- 020223/201

0-1

1-2

2-3

3-4 4-5 Page **116** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low- privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges. CVE ID : CVE-2023- 20010					
Vendor: clas	ssroombookin	gs		L				
Product: cla	ssroombookir	igs						
Affected Ver	sion(s): 2.6.4				-			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in craigrodway classroombookings 2.6.4 allows attackers to execute arbitrary code or other unspecified impacts via the input bgcol in file Weeks.php. CVE ID : CVE-2023- 23012	N/A	A-CLA-CLAS- 020223/202			
Vendor: contec								
Product: conprosys_hmi_system								
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 117 of 463	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): * Up to (including) 3.4.5								
Improper Privilege Manageme nt	20-Jan-2023	7.5	Use of default credentials vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote unauthenticated attacker to alter user credentials information. CVE ID : CVE-2023- 22331	https://jvn.jp /en/vu/JVNV U96873821, https://www. contec.com/d ownload/cont ract/contract 4/?itemid=ea 8039aa-3434- 4999-9ab6- 897aa690210 c&downloadit emid=866d7d 3c-aae9- 438d-87f3- 17aa040df90 b	A-CON- CONP- 020223/203			
N/A	20-Jan-2023	7.5	Improper access control vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote unauthenticated attacker to bypass access restriction and obtain the server certificate including the private key of the product. CVE ID : CVE-2023- 22339	https://jvn.jp /en/vu/JVNV U96873821, https://www. contec.com/d ownload/cont ract/contract 4/?itemid=ea 8039aa-3434- 4999-9ab6- 897aa690210 c&downloadit emid=866d7d 3c-aae9- 438d-87f3- 17aa040df90 b	A-CON- CONP- 020223/204			
Improper Neutralizat ion of Input During Web Page Generation	20-Jan-2023	5.4	Cross-site scripting vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote authenticated attacker to inject an arbitrary script and	https://jvn.jp /en/vu/JVNV U96873821, https://www. contec.com/d ownload/cont ract/contract 4/?itemid=ea	A-CON- CONP- 020223/205			

0-1

1-2

2-3 3-4 4-5 Page **118** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			obtain the sensitive information. CVE ID : CVE-2023- 22373	8039aa-3434- 4999-9ab6- 897aa690210 c&downloadit emid=866d7d 3c-aae9- 438d-87f3- 17aa040df90 b	
Improper Authentica tion	20-Jan-2023	5.3	Use of password hash instead of password for authentication vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote authenticated attacker to obtain user credentials information via a man-in-the-middle attack. CVE ID : CVE-2023- 22334	https://jvn.jp /en/vu/JVNV U96873821, https://www. contec.com/d ownload/cont ract/contract 4/?itemid=ea 8039aa-3434- 4999-9ab6- 897aa690210 c&downloadit emid=866d7d 3c-aae9- 438d-87f3- 17aa040df90 b	A-CON- CONP- 020223/206
Vendor: cus	tom_404_pro_	project			
Product: cu	stom_404_pro				
Affected Ver	sion(s): * Up to	(excluding	g) 3.7.2		
Cross-Site Request Forgery (CSRF)	18-Jan-2023	4.3	The Custom 404 Pro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.7.1. This is due to missing or incorrect nonce validation on the custom_404_pro_admin _init function. This makes it possible for unauthenticated	https://plugin s.trac.wordpr ess.org/brows er/custom- 404- pro/tags/3.7. 1/admin/Ad minClass.php #L114, https://www. wordfence.co m/threat- intel/vulnera	A-CUS-CUST- 020223/207

0-1

1-2

2-3 3-4 4-5 Page **119** of **463** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to delete logs, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	bilities/id/96 8920b9-febf- 4d76-a16b- f27954cd72e 5	
			CVE ID : CVE-2023- 0385		
Vendor: daj				L	
Product: m-	filter				
Affected Ver	sion(s): From (i	ncluding)	4.0 Up to (excluding) 4.87	r04	
N/A	17-Jan-2023	5.3	m-FILTER prior to Ver.5.70R01 (Ver.5 Series) and m-FILTER prior to Ver.4.87R04 (Ver.4 Series) allows a remote unauthenticated attacker to bypass authentication and send users' unintended email when email is being sent under the certain conditions. The attacks exploiting this vulnerability have been observed. CVE ID : CVE-2023- 22278	N/A	A-DAJ-M-FI- 020223/208
Affected Ver	sion(s): From (i	ncluding)	5.0 Up to (excluding) 5.70	r01	
N/A	17-Jan-2023	5.3	m-FILTER prior to Ver.5.70R01 (Ver.5 Series) and m-FILTER prior to Ver.4.87R04 (Ver.4 Series) allows a remote unauthenticated attacker to bypass authentication and send users' unintended email when email is being sent under the certain	N/A	A-DAJ-M-FI- 020223/209

0-1

1-2

2-3 3-4 4-5 Page **120** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			conditions. The attacks exploiting this vulnerability have been observed.					
			CVE ID : CVE-2023- 22278					
Vendor: dal	oradius			1	1			
Product: da	loradius							
Affected Vers	sion(s): * Up to	(excluding	g) 2023-01-18					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository lirantal/daloradius prior to master-branch. CVE ID : CVE-2023- 0337	https://huntr. dev/bounties /1c50a5a5- 3f55-4b6f- b861- 4d5cdb6eb81 b, https://githu b.com/lirantal /daloradius/c ommit/e77a7 69c7503e63a 2e3c05262cb 5f8f81a4a7bb e	A-DAL-DALO- 020223/210			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository lirantal/daloradius prior to master-branch. CVE ID : CVE-2023- 0338	https://huntr. dev/bounties /fcae1b67- db37-4d24- 9137- 8dda95573e7 7, https://githu b.com/lirantal /daloradius/c ommit/e77a7 69c7503e63a 2e3c05262cb 5f8f81a4a7bb e	A-DAL-DALO- 020223/211			
Vendor: Dell								
Product: cloud_mobility_for_dell_emc_storage								
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			
			Page 121 of 463					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): * Up to (excluding) 1.3.4.0								
Improper Certificate Validation	19-Jan-2023	7	Cloud Mobility for Dell EMC Storage, versions 1.3.0.X and below contains an Improper Check for Certificate Revocation vulnerability. A threat actor does not need any specific privileges to potentially exploit this vulnerability. An attacker could perform a man-in-the-middle attack and eavesdrop on encrypted communications from Cloud Mobility to Cloud Storage devices. Exploitation could lead to the compromise of secret and sensitive information, cloud storage connection downtime, and the integrity of the connection to the Cloud devices. CVE ID : CVE-2023- 23690	https://www. dell.com/supp ort/kbdoc/en - us/00020752 1/dsa-2023- 019-dell-emc- cloud- mobility- security- update-for- certificate- revocation- vulnerability	A-DEL-CLOU- 020223/212			
Vendor: der	10	<u>.</u>		<u> </u>				
Product: de	no							
Affected Ver	sion(s): From (i	ncluding)	1.9.0 Up to (excluding) 1.2	.9.3				
Concurrent Execution using Shared Resource with Improper Synchroniz ation	17-Jan-2023	7.5	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Multi-threaded programs were able to spoof interactive permission prompt by rewriting the prompt to	https://githu b.com/denola nd/deno/pull /17392	A-DEN- DENO- 020223/213			

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4

4-5

5-6

6-7

7-8

8-9

('Race Condition')suggest that program is waiting on user confirmation to unrelated action. A malicious program could clear the terminal screen after permission prompt was shown and write a generic message. This situation impacts users who use Web Worker API and relied on interactive permission prompt. The reproduction is very timing sensitive and can't be reliably reproduced on every try. This problem can not be exploited on systems that do not attach an interactive prompt (for example headless servers). The problem has been fixed in Deno v1.29.3; it is recommende all users update to this version. Users are advised to upgrade. Users unable to disable interactive permission prompts. CVE ID : CVE-2023- 22499Ittps://devolA-DEV- REMO- N/AVendor: de-viewterJ.3.0The force offline MFA promy respected whenhttps://devolA-DEV- REMO- 020223/214	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A26-Jan-20233.3The force offline MFA promy setting is nothttps://devolN/A26-Jan-20233.3The force offline MFA promy setting is nothttps://devolA-DEV- REMO-	('Race	Publish Date	CVSSv3	suggest that program is waiting on user confirmation to unrelated action. A malicious program could clear the terminal screen after permission prompt was shown and write a generic message. This situation impacts users who use Web Worker API and	Patch	NCIIPC ID
N/A26-Jan-20233.3The force offline MFA prompt setting is nothttps://devol prompt setting is notA-DEV- REMO- recome 1000000000000000000000000000000000000				permission prompt. The reproduction is very timing sensitive and can't be reliably reproduced on every try. This problem can not be exploited on systems that do not attach an interactive prompt (for example headless servers). The problem has been fixed		
Vendor: devolutionsProduct: remote_desktop_managerAffected Version(s): 2022.3.29N/A26-Jan-20233.3The force offline MFA prompt setting is nothttps://devol utions.net/secA-DEV- REMO- 000000000000000000000000000000000000				recommended all users update to this version. Users are advised to upgrade. Users unable to upgrade may run withno-prompt flag to disable interactive permission prompts. CVE ID : CVE-2023-		
Product: remote_desktop_manager Affected Version(s): 2022.3.2 N/A 26-Jan-2023 3.3 The force offline MFA prompt setting is not https://devol utions.net/sec A-DEV-REMO- N/A 26-Jan-2023 3.3 The force offline MFA prompt setting is not https://devol utions.net/sec A-DEV-				22499		
Affected Version(s): 2022.3.29 N/A 26-Jan-2023 3.3 The force offline MFA prompt setting is not https://devol utions.net/sec A-DEV-REMO-	Vendor: dev	olutions				
N/A 26-Jan-2023 3.3 The force offline MFA prompt setting is not utions.net/sec REMO-	Product: re	mote_desktop_	manager			
N/A 26-Jan-2023 3.3 prompt setting is not utions.net/sec REMO-	Affected Ver	sion(s): 2022.3.	29			
	N/A	26-Jan-2023	3.3	prompt setting is not	utions.net/sec	REMO-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	/-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switching to offline mode in Devolutions Remote Desktop Manager 2022.3.29 to 2022.3.30 allows a user to save sensitive data on disk. CVE ID : CVE-2023-	es/DEVO- 2023-0001	
			0463		
Affected Ver	sion(s): 2022.3.	30			
N/A	26-Jan-2023	3.3	The force offline MFA prompt setting is not respected when switching to offline mode in Devolutions Remote Desktop Manager 2022.3.29 to 2022.3.30 allows a user to save sensitive data on disk. CVE ID : CVE-2023- 0463	https://devol utions.net/sec urity/advisori es/DEVO- 2023-0001	A-DEV- REMO- 020223/215
Vendor: e-d	ynamics				
Product: ev	ents_made_eas	S y			
Affected Ver	sion(s): * Up to	(including	g) 2.3.16		
Missing Authorizati on	19-Jan-2023	5.4	The Events Made Easy plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on several functions related to AJAX actions in versions up to, and including, 2.3.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke those functions intended for	https://plugin s.trac.wordpr ess.org/chang eset?sfp_email =&sfph_mail= &reponame= &old=283630 8%40events- made- easy&new=28 36308%40ev ents-made- easy&sfp_ema il=&sfph_mail =	A-E-D-EVEN- 020223/216

0-1

1-2

2-3

3-4 4-5 Page **124** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator use. While the plugin is still pending review from the WordPress repository, site owners can download a copy of the patched version directly from the developer's Github at https://github.com/lied ekef/events-made-easy CVE ID : CVE-2023-		
			0404		
Vendor: eco	mmerce-code	igniter-bo	ootstrap_project		
	ommerce-code	0	-		
Affected Ver	sion(s): * Up to	(excludinរ្	g) 2022-12-27		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in Ecommerce- CodeIgniter-Bootstrap thru commit d5904379ca55014c5df 34c67deda982c73dc7fe 5 (on Dec 27, 2022), allows attackers to execute arbitrary code via the languages and trans_load parameters in file add_product.php. CVE ID : CVE-2023- 23010	https://githu b.com/kirilkir kov/Ecommer ce- CodeIgniter- Bootstrap/co mmit/d59043 79ca55014c5 df34c67deda9 82c73dc7fe5, https://githu b.com/kirilkir kov/Ecommer ce- CodeIgniter- Bootstrap/iss ues/242, https://gist.gi thub.com/enf eras/8a83600 8e9f635a2f80 d09c9a8b5a5 33	A-ECO- ECOM- 020223/217
Vendor: Fro					
Product: fro	DXIOT				

0-1

1-2

2-3

3-44-5Page 125 of 463

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.0		
Path Traversal: 'filename'	16-Jan-2023	5.5	Path Traversal: '\\filename' in GitHub repository froxlor/froxlor prior to 2.0.0. CVE ID : CVE-2023- 0316	https://githu b.com/froxlor /froxlor/com mit/983d929 46039250182 25d672795bd 8b4a526f41e, https://huntr. dev/bounties /c190e42a- 4806-47aa- aa1e- ff5d6407e244	A-FRO-FROX- 020223/218
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.8		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	16-Jan-2023	8.8	Command Injection in GitHub repository froxlor/froxlor prior to 2.0.8. CVE ID : CVE-2023- 0315	https://huntr. dev/bounties /ff4e177b- ba48-4913- bbfa- ab8ce0db594 3, https://githu b.com/froxlor /froxlor/com mit/090cfc26 f2722ac3036c c7fd1861955 bc36f065a	A-FRO-FROX- 020223/219
Vendor: full	worksplugins				
Product: qu	ick_event_man	ager			
Affected Ver	sion(s): * Up to	(excludin	g) 9.7.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	The Quick Event Manager WordPress Plugin, version < 9.7.5, is affected by a reflected cross-site scripting vulnerability in the 'category' parameter of its 'qem_ajax_calendar' action.	N/A	A-FUL-QUIC- 020223/220

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 23491							
Vendor: Glp	oi-project									
Product: glpi										
Affected Ver	Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.6									
Incorrect Authorizati on	26-Jan-2023	7.5	GLPI is a Free Asset and IT Management Software package. Versions 10.0.0 and above, prior to 10.0.6 are vulnerable to Incorrect Authorization. This vulnerability allow unauthorized access to inventory files. Thus, if anonymous access to FAQ is allowed, inventory files are accessbile by unauthenticated users. This issue is patched in version 10.0.6. As a workaround, disable native inventory and delete inventory files from server (default location is `files/_inventory`). CVE ID : CVE-2023- 22500	N/A	A-GLP-GLPI- 020223/221					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2023	6.1	GLPI is a Free Asset and IT Management Software package. Versions 9.4.0 and above, prior to 10.0.6 are subject to Cross-site Scripting. An attacker can persuade a victim into opening a URL containing a payload exploiting this vulnerability. After	N/A	A-GLP-GLPI- 020223/222					

0-1

1-2

2-3

3-4 4-5 Page **127** of **463** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited, the attacker can make actions as the victim or exfiltrate session cookies. This issue is patched in version 10.0.6.		
			CVE ID : CVE-2023- 22722		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2023	4.8	GLPI is a Free Asset and IT Management Software package. Versions prior to 10.0.6 are subject to Cross-site Scripting via malicious RSS feeds. An Administrator can import a malicious RSS feed that contains Cross Site Scripting (XSS) payloads inside RSS links. Victims who wish to visit an RSS content and click on the link will execute the Javascript. This issue is patched in 10.0.6. CVE ID : CVE-2023- 22724	N/A	A-GLP-GLPI- 020223/223
Affected Ver	sion(s): From (i	ncluding)	9.4.0 Up to (excluding) 9.5	5.12	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2023	6.1	GLPI is a Free Asset and IT Management Software package. Versions 9.4.0 and above, prior to 10.0.6 are subject to Cross-site Scripting. An attacker can persuade a victim into opening a URL containing a payload exploiting this vulnerability. After exploited, the attacker	N/A	A-GLP-GLPI- 020223/224

0-1

1-2

2-33-44-5Page 128 of 463

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can make actions as the victim or exfiltrate session cookies. This issue is patched in version 10.0.6.		
			CVE ID : CVE-2023- 22722		
Vendor: gpa	ac				
Product: gp	ac				
Affected Ver	sion(s): * Up to	(including	g) 2.2.0		
Use After Free	18-Jan-2023	7.8	Use After Free in GitHub repository gpac/gpac prior to 2.3.0-DEV. CVE ID : CVE-2023- 0358	https://huntr. dev/bounties /93e128ed- 253f-4c42- 81ff- fbac7fd8f355, https://githu b.com/gpac/g pac/commit/ 9971fb125cf9 1cefd081a080 c417b90bbe4 a467b	A-GPA-GPAC- 020223/225
Affected Ver	sion(s): 2.2-rev	0-gab0121	bbfb-master		
Missing Release of Memory after Effective Lifetime	20-Jan-2023	7.8	GPAC version 2.2-rev0- gab012bbfb-master was discovered to contain a memory leak in lsr_read_rare_full function. CVE ID : CVE-2023- 23145	https://githu b.com/gpac/g pac/commit/ 4ade98128cb c41d5115b97 a41ca2e5952 9c8dd5f	A-GPA-GPAC- 020223/226
Integer Overflow or Wraparoun d	20-Jan-2023	5.5	Integer overflow vulnerability in function Q_DecCoordOnUnitSph ere file bifs/unquantize.c in GPAC version 2.2-rev0- gab012bbfb-master.	https://githu b.com/gpac/g pac/commit/ 3a2458a49b3 e6399709d45 6d7b35e7a6f 50cfb86	A-GPA-GPAC- 020223/227

0-1

1-2

2-3 3-4 4-5 Page **129** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23144		
Affected Ver	sion(s): 2.3-dev	-rev1-g46	69ba229-master		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-2023	7.8	Buffer overflow vulnerability in function avc_parse_slice in file media_tools/av_parsers .c. GPAC version 2.3- DEV-rev1-g4669ba229- master. CVE ID : CVE-2023- 23143	https://githu b.com/gpac/g pac/commit/ af6a5e7a96ee 01a139cce6c9 e4edfc069aad 17a6	A-GPA-GPAC- 020223/228
Vendor: hea	althchecks			1	
Product: he	althchecks				
Affected Ver	sion(s): * Up to	(excluding	g) 2.6		
Observable Discrepanc y	23-Jan-2023	5.3	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository healthchecks/healthche cks prior to v2.6. CVE ID : CVE-2023- 0440	https://huntr. dev/bounties /208a096f- 7986-4eed- 8629- b7285348a68 6, https://githu b.com/healthc hecks/healthc hecks/commit /359edbd270 9e27b606870 61a32e19322 bc971c1f	A-HEA- HEAL- 020223/229
Vendor: htm	nl-stripscripts	project			
	ml-stripscripts				
Affected Ver	sion(s): * Up to	(including	g) 1.06		
N/A	21-Jan-2023	7.5	The HTML-StripScripts module through 1.06 for Perl allows _hss_attval_style ReDoS because of catastrophic backtracking for HTML	N/A	A-HTM- HTML- 020223/230

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Unauthoriz ed ActorInstance (additional sequence interplane interp	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Vendor: IBMProduct: qradar_security_information_and_event_managerAffected Version(s): 7.4.0Exposure of Sensitive Information to an Unauthoriz ed ActorIsta and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 2875https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244356. CVE ID : CVE-2023- 2875A-IBM- QRAD- 020223/23Affected Version(s): 7.5.0IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that that do not requi				style attributes.				
Product: qradar_security_information_and_event_managerAffected Version(s): 7.4.0Exposure of Sensitive Information n to an Unauthoriz ed Actor17-Jan-20237.5IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356.https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244356.Affected Version(s): 7.5.0IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that do for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that do require that key. IBM X-Force ID: 244356.https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244356.Affected Version(s): 7.5.07.5IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356.https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244356.Product: robite_process_autemationIBM Robotic Process Automation 20.12.0https://www. ibm.com/sup port/pages/n ode/6855643Affected Version(s): * Up to (excluding) 21.0.2 defaults on of Sensitive Informatio n18-Jan-20235.9IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitlyhttps://excha nge.xforce.ibCleartext Transmi				24038				
Affected Version(s): 7.4.0IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.xforce.ib mcloud.com/v ulmerabilities/ 244356. 0de/6855643A-IBM- QRAD- 020223/23Affected Version(s): 7.5.0IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.xforce.ib mcloud.com/v ulmerabilities/ 244356. 0de/6855643Affected Version(s): 7.5.0IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875A-IBM- QRAD- 020223/23Product: robustic process_automationIBM Robotic Process Automation 20.12.0 through 21.0.2 defaults port/pages/n ode/685543A-IBM- QRAD- 020223/23Affected Version(s): * Up to (excluding) 21.0.3IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults port/pages/n ode/6855643A-IBM-ROB 020223/23	Vendor: IBM	1						
Exposure of Sensitive Information to an Unauthoriz ed ActorI.7-Jan-2023Z.5IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.xforce.ib mcloud.com/v ulmerabilities/ 244356. CVE ID : CVE-2023- 22875https://www. port/pages/n ode/6855643A-IBM- QRAD- 020223/23Affected Version(s): 7.5.0IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.xforce.ib mcloud.com/v ulmerabilities/ 244356. CVE ID : CVE-2023- 22875Product: robust Cleartext Transmissi on of Sensitive Information n18-Jan-20235.9IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitlyhttps://www. ibm.com/sup port/pages/n ode/6855643A-IBM-ROB 020223/23	Product: qra	adar_security_	informat	ion_and_event_manager				
Exposure of Sensitive Information n to an Unauthoriz ed Actor17-Jan-20237.5and 7.5copies certificate key files used for SL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.Xforce.ib mcloud.com/v ulnerabilities/ 244356.A-IBM- QRAD- (DRAD- QRAD- (DRAD- QRAD- Mither interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.Xforce.ib mcloud.com/v ulnerabilities/ 244356.A-IBM- QRAD- QRAD- Mither interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.Xforce.ib mcloud.com/v ulnerabilities/ 244356. Mithps://www. de/6855643A-IBM- QRAD- QRAD- Mither interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.Xforce.ib mcloud.com/v ulnerabilities/ 244356. Mithps://www. de/6855643A-IBM- QRAD- QRAD- QRAD- QRAD- QRAD- QRAD- Q20223/23Product:rot-cryJIT-Jan-2023 SF.SIBM Robotic Process Automation 20.12.0 through 21.0.2 defaults ode/6855837, https://excha node/6855837, https://excha port/pages/n ode/6855837, https://excha port/pages/n ode/6855837, https://excha port/pages/n ode/6855837, https://excha port/pages/n ode/6855837, https://excha port/pages/n ode/6855837, https://excha port/pages/n ode/6855837, https://excha <b< td=""><td>Affected Vers</td><td>sion(s): 7.4.0</td><td></td><td></td><td></td><td></td></b<>	Affected Vers	sion(s): 7.4.0						
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor17-Jan-2023 17-Jan-20237.5IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ QRAD- 020223/23Product: ro-tro-tro-tro-tro-tro-tro-tro-tro-tro-t	of Sensitive Informatio n to an Unauthoriz	17-Jan-2023	7.5	and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023-	nge.xforce.ib mcloud.com/v ulnerabilities/ 244356, https://www. ibm.com/sup port/pages/n			
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor17-Jan-20237.54and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356.https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244356, https://www. ibm.com/sup port/pages/n ode/6855643A-IBM- QRAD- 020223/23 020223/23 ibm.com/sup port/pages/n ode/6855643Product: rote-tro	Affected Vers	sion(s): 7.5.0			I			
Affected Version(s): * Up to (excluding) 21.0.3 Cleartext Transmissi on of Sensitive Informatio n Informatio 18-Jan-2023 5.9 Informatio 10 18-Jan-2023 5.9 Informatio 10 10 10 10 10 10 10 10 10 10 10 10 11 11 11 12	of Sensitive Informatio n to an Unauthoriz ed Actor	-		and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875	nge.xforce.ib mcloud.com/v ulnerabilities/ 244356, https://www. ibm.com/sup port/pages/n			
Cleartext Transmissi on of Sensitive Informatio18-Jan-2023IBM Robotic Process Automation 20.12.0https://www. ibm.com/sup port/pages/n ode/6855837, https://excha nA-IBM-ROB 020223/23Informatio n18-Jan-20235.9IBM Robotic Process Automation 20.12.0https://pages/n ode/6855837, https://excha nge.xforce.ibA-IBM-ROB 020223/23		-						
Transmissi on of Sensitive Informatio18-Jan-20235.9Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA ortexplicitlyibm.com/sup port/pages/n ode/6855837, https://excha 	Affected Version(s): * Up to (excluding) 21.0.3							
	Transmissi on of Sensitive Informatio	18-Jan-2023	5.9	Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the	ibm.com/sup port/pages/n ode/6855837, https://excha	A-IBM-ROBO- 020223/233		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1	CVSS Scoring S	icale 0-1	1-2 7	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X- Force ID: 244109.	mcloud.com/v ulnerabilities/ 244109	
			CVE ID : CVE-2023- 22863		
Affected Ver	sion(s): * Up to	(excluding	g) 21.0.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 244075. CVE ID : CVE-2023- 22594	https://www. ibm.com/sup port/pages/n ode/6855835, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244075	A-IBM-ROBO- 020223/234
Product: ro	botic_process_	automati	on_as_a_service		
Affected Ver	sion(s): * Up to	(excluding	g) 21.0.3		
Cleartext Transmissi on of Sensitive Informatio n	18-Jan-2023	5.9	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle	https://www. ibm.com/sup port/pages/n ode/6855837, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244109	A-IBM-ROBO- 020223/235

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			techniques. IBM X- Force ID: 244109.			
			CVE ID : CVE-2023- 22863			
Affected Vers	sion(s): * Up to	(excluding	g) 21.0.5			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 244075. CVE ID : CVE-2023- 22594	https://www. ibm.com/sup port/pages/n ode/6855835, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244075	A-IBM-ROBO- 020223/236	
	botic_process_s sion(s): * Up to		on_for_cloud_pak			
Allected vers		(excluding		[
Cleartext Transmissi on of Sensitive Informatio18-Jan-2023IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA prefix is not explicitly specified in the URL. This could allow an attacker to obtain sensitive information nhttps://www. ibm.com/sup port/pages/n ode/6855837, https://excha nge.xforce.ib mcloud.com/v using man in the middle ulnerabilities/ 244109A-IBM-RC 020223/2CVE ID : CVE-2023- 22863CVE ID : CVE-2023- 22863A-IBM-RC mcloud.com/v						
Affected Vers	sion(s): * Up to	(excluding	g) 21.0.5			

0-1

1-2

2-3

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 244075. CVE ID : CVE-2023-	https://www. ibm.com/sup port/pages/n ode/6855835, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244075	A-IBM-ROBO- 020223/238				
			22594						
Affected Ver	Affected Version(s): From (including) 21.0.1 Up to (excluding) 21.0.5								
Incorrect Permission Assignmen t for Critical Resource	18-Jan-2023	7.8	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.4 could allow a local user to perform unauthorized actions due to insufficient permission settings. IBM X-Force ID: 244073. CVE ID : CVE-2023- 22592	https://www. ibm.com/sup port/pages/n ode/6855839, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244073	A-IBM-ROBO- 020223/239				
Vendor: inv	Vendor: inventory_system_project								
Product: inv	ventory_system	1							
Affected Ver	sion(s): * Up to	(including	g) 2021-04-23						
Improper Neutralizat ion of Input During Web Page Generation	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in InventorySystem thru commit e08fbbe179021463135 01ed0b5feba81d58f45 5c (on Apr 23, 2021) via edit_store_name and	N/A	A-INV-INVE- 020223/240				

CVSS Scoring Scale0-11-22-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
('Cross-site Scripting')			edit_active inputs in file InventorySystem.php. CVE ID : CVE-2023- 23014						
Vendor: jc2	1								
Product: nginx_proxy_manager									
Affected Version(s): * Up to (including) 2.9.19									
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	8.8	jc21 NGINX Proxy Manager through 2.9.19 allows OS command injection. When creating an access list, the backend builds an htpasswd file with crafted username and/or password input that is concatenated without any validation, and is directly passed to the exec command, potentially allowing an authenticated attacker to execute arbitrary commands on the system. NOTE: this is not part of any NGINX software shipped by F5. CVE ID : CVE-2023- 23596	N/A	A-JC2-NGIN- 020223/241				
	kun_project								
Product: ka									
Affected Ver	<mark>sion(s): 0.8.0</mark>			https://gist.gi					
Improper Neutralizat ion of Input During Web Page Generation	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in Kalkun 0.8.0 via username input in file User_model.php. CVE ID : CVE-2023- 23015	https://gist.gi thub.com/enf eras/eaf5991 90451745f1b 339f64cca4a3 6d, https://githu b.com/kalkun -	A-KAL-KALK- 020223/242				
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 135 of 463									

Scripting')ssues/487Secripting')Sues/487Vendor: KeepassAffected Version(s): * Up to (including) 2.53Affected Version(s): * Up to (including) 2.53(in a default installation) allows an attacker, who has write access to the XML configuration file, to obtain the cleartext passwords by adding an export trigger. NOTE: the vendor's position is hat the password database is not intended to be secure against an attacker who has that level of access to the local PC.https://sourc eforge.net/p/ keepass/discu password database is not intended to be secure against an attacker who has that level of access to the local PC.A-KEE-KEEP- 020223/243Vendor: libgit2Product: libgit2Mathematication of Cit When using an SSII remote with the optional libssh2 hic20-Jan-20235.9Ibigit2 is a cross- platform, linkable library implementation of Git When using an SSII remote with the optional libssh2 backend, libgit2 does not perform certificate checking by default.https://githu b.com/libgit220-Jan-20235.9S.9Backend, libgit2 does not perform certificate checking by default.https://githu b.com/libgit2	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: keepassAffected Version(s): * Up to (including) 2.53Affected Version(s): * Up to (including) 2.53Improper of Sensitive Information22-Jan-20235.55.65.55.75.7 </td <td>('Cross-site Scripting')</td> <td></td> <td></td> <td></td> <td></td> <td></td>	('Cross-site Scripting')									
Affected Version(s): * Up to (including) 2.53Cleartext Storage of Sensitive Informatio 	Vendor: Keepass									
Cleartext Storage of Sensitive n22-Jan-20235.5** DISPUTED ** KeePass through 2.53 (in a default installation) allows an attacker, who has write access to the XML configuration file, to obtain the cleartext passwords by adding an export trigger. NOTE: the vendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC.https://sourc eforge.net/p/ keepass/discu sion/329220 /thread/1416 e5cf6b/A-KEE-KEEP- 020223/2433Vendor: libgit2Evendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC.https://sourc eforge.net/p/ keepass/discu sion/329220 /thread/1416 e5cf6b/A-KEE-KEEP- 020223/2433Vendor: libgit2Evendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC.https://githu b.com/libgit2 /libgit2/com mit/42e5db9 Bb963ae5032 29c63e44e06 A-LIB-LIBG- 020223/244Improper Verificatio n of cryptograp hic Signature20-Jan-20235.9libgit2 is a cross- platform, linkable library implementation of Git. When using an SSH remote with the optional libssh2 eady of default. Prior versions of libgit2 require the caller to set the 'certificate_check' field of libgit2'sA-LIB-LIBG- 020223/244	Product: ke	epass								
Cleartext Storage of Sensitive Information22-Jan-20235.5KeePass through 2.53 (in a default installation) allows an attacker, who has write access to the XML configuration file, to obtain the cleartext passwords by adding an export trigger. NOTE: the vendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC. CVE ID : CVE-2023- 24055https://sourc eforge.net/p/ keepass/discu ssion/329220 /thread/a146 e5cf6b/A-KEE-KEEP- 020223/243Vendor: libgit2Jumproper verification n of Cryptograp hic SignatureJumproper S9.9Ittps://sithu patform, linkable library implementation of Git. When using an SSH remote with the optional libssh2 mot perform certificate checking by default. Prior versions of libgit2 (libgit2/com mit/42e5db9 B0963ae5032 29c63e44e06 e439f50e56, https://githu b.com/libgit2 (libgit2/com mit/42e5db9 B0963ae5032 29c63e44e06 e439f50e56, https://githu b.com/libgit2 (libgit2/com mit/42e5db9 B0963ae5032 29c63e44e06 e439f50e56, https://githu b.com/libgit2 (libgit2/com mit/42e5db9 B0963ae5032 29c63e44e06 e439f50e56, https://githu b.com/libgit2 (libgit2/com mit/42e5db9 B0963ae5032 29c63e44e06 e439f50e56, https://githu b.com/libgit2 (libgit2/com mit/42e5db9 B0963ae5032 29c63e44e06 e439f50e56, https://githu b.com/libgit2 (libgit2/com mit/42e5db9 B0963ae5032 29c63e44e06 e439f50e56, https://githu b.com/libgit2 (libgit2/com mit/42e5db9A-LIB-LIBG- 020223/244	Affected Ver	sion(s): * Up to	(including	g) 2.53						
Product: libgit2Affected Version(s): * Up to (excluding) 1.4.5Affected Version(s): * Up to (excluding) 1.4.5Improper Verificatio n of Cryptograp hic SignatureIbigit2 is a cross- platform, linkable libgit2/com of Git. When using an SSH remote with the optional libssh2 backend, libgit2 does not perform certificate checking by default.https://githu b.com/libgit2 /libgit2/com mit/42e5db9 8b963ae5032 29c63e44e06 e439df50e56, https://githu b.com/libgit2 /libgit2/com mit/cd6f679a f401eda1f172A-LIB-LIBG- 020223/244	Cleartext Storage of Sensitive Informatio n	22-Jan-2023	5.5	KeePass through 2.53 (in a default installation) allows an attacker, who has write access to the XML configuration file, to obtain the cleartext passwords by adding an export trigger. NOTE: the vendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC. CVE ID : CVE-2023-	eforge.net/p/ keepass/discu ssion/329220 /thread/a146					
Affected Version(s): * Up to (excluding) 1.4.5Affected Version(s): * Up to (excluding) 1.4.5Improper Verificatio n of Cryptograp hic Signaturelibgit2 is a cross- platform, linkable library implementation of Git. When using an SSH remote with the optional libssh2 backend, libgit2 does not perform certificate checking by default. Prior versions of libgit2 require the caller to set the `certificate_check` field of libgit2'shttps://githu b.com/libgit2 A-LIB-LIBG- 020223/244	Vendor: libg	git2								
Improper Verificatio n of Cryptograp hic Signature20-Jan-20235.9Ibigit2 is a cross- platform, linkable library implementation of Git. When using an SSH remote with the 	Product: lib	git2								
Improper Verificatio n of Cryptograp hic Signature20-Jan-20235.9platform, linkable library implementation of Git. When using an backend, libgit2 does not perform certificate checking by default.b.com/libgit2 /libgit2/com mit/42e5db9 8b963ae5032 29c63e44e06 e439df50e56, https://githu b.com/libgit220-Jan-20235.9backend, libgit2 does not perform certificate checking by default.A-LIB-LIBG- 020223/244Verificatio ic Signatureprior versions of libgit2 require the caller to set the `certificate_check` field of libgit2's/libgit2/com mit/cd6f679a f401eda1f172	Affected Ver	sion(s): * Up to	(excluding	g) 1.4.5						
	Improper Verificatio n of Cryptograp hic Signature20-Jan-20235.9platform, linkable library implementation of Git. When using an optional libssh2 backend, libgit2 does not perform certificate checking by default.b.com/libgit2 /libgit2/com e439df50e56, https://githu b.com/libgit2A-LIB-LIBG- 020223/244020-Jan-20235.95.9backend, libgit2 does not perform certificate checking by default.https://githu b.com/libgit2A-LIB-LIBG- 020223/2441005.9Frior versions of libgit2 require the caller to set the `certificate_check` field of libgit2'sHttps://githu 402006ef826A-LIB-LIBG- 020223/244									
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure - if a certificate check callback is not set, libgit2 does not perform any certificate checking. This means that by default - without configuring a certificate check callback, clients will not perform validation on the server SSH keys and may be subject to a man-in-the-middle attack. Users are encouraged to upgrade to v1.4.5 or v1.5.1. Users unable to upgrade should ensure that all relevant certificates are manually checked.		
			CVE ID : CVE-2023- 22742		
Affected Ver	sion(s): 1.5.0				
Improper Verificatio n of Cryptograp hic Signature	20-Jan-2023	5.9	libgit2 is a cross- platform, linkable library implementation of Git. When using an SSH remote with the optional libssh2 backend, libgit2 does not perform certificate checking by default. Prior versions of libgit2 require the caller to set the `certificate_check` field of libgit2's `git_remote_callbacks` structure - if a certificate check callback is not set, libgit2 does not	https://githu b.com/libgit2 /libgit2/com mit/42e5db9 8b963ae5032 29c63e44e06 e439df50e56, https://githu b.com/libgit2 /libgit2/com mit/cd6f679a f401eda1f172 402006ef826 5f8bd58ea	A-LIB-LIBG- 020223/245

0-1

1-2

2-3

3-4 4-5 Page **137** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			perform any certificate checking. This means that by default - without configuring a certificate check callback, clients will not perform validation on the server SSH keys and may be subject to a man-in-the-middle attack. Users are encouraged to upgrade to v1.4.5 or v1.5.1. Users unable to upgrade should ensure that all relevant certificates are manually checked.				
			CVE ID : CVE-2023- 22742				
Vendor: ligh	ntftp_project						
Product: lig	•						
Affected Ver	sion(s): * Up to	(including		1			
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	21-Jan-2023	7.5	A race condition in LightFTP through 2.2 allows an attacker to achieve path traversal via a malformed FTP request. A handler thread can use an overwritten context- >FileName. CVE ID : CVE-2023- 24042	N/A	A-LIG-LIGH- 020223/246		
Vendor: login_with_phone_number_project							
Product: login_with_phone_number							
Affected Version(s): * Up to (excluding) 1.4.2							
Improper Neutralizat ion of Special	20-Jan-2023	8.8	The Login with Phone Number WordPress Plugin, version < 1.4.2, is affected by an	N/A	A-LOG-LOGI- 020223/247		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 138 of 463	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			authenticated SQL injection vulnerability in the 'ID' parameter of its 'lwp_forgot_password' action.		
			CVE ID : CVE-2023- 23492		
Vendor: ma	tbao				
Product: wp	o_helper_prem	ium			
Affected Ver	sion(s): * Up to	(excluding	g) 4.3		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	26-Jan-2023	6.1	The WP Helper Lite WordPress plugin, in versions < 4.3, returns all GET parameters unsanitized in the response, resulting in a reflected cross-site scripting vulnerability.	N/A	A-MAT- WP_H- 020223/248
Scripting')			CVE ID : CVE-2023- 0448		
Vendor: Me					
Product: me					
Affected Ver	sion(s): * Up to	(excluding		Γ	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	5.4	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time- precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally	https://phabr icator.wikime dia.org/T323 592	A-MED- MEDI- 020223/249

0-1

1-2

2-33-44-5Page 139 of 463

5-6

		have the editsitejs capability.		
		CVE ID : CVE-2023- 22910		
20-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES- CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt.	https://phabr icator.wikime dia.org/T315 123	A-MED- MEDI- 020223/250
		CVE ID : CVE-2023- 22912		
ion(s): 1.39.0				
20-Jan-2023	5.4	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time- precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally have the editsitejs capability. CVE ID : CVE-2023-	https://phabr icator.wikime dia.org/T323 592	A-MED- MEDI- 020223/251
i	on(s): 1.39.0	on(s): 1.39.0	20-Jan-2023An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES- CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt. CVE ID : CVE-2023- 22912 on(s): 1.39.0An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time- precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally have the editsitejs capability.	20-Jan-20235.3An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES- CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt.https://phabr icator.wikime dia.org/T315 123on(s): 1.39.0An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time- precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally have the editsitejs capability.https://phabr icator.wikime dia.org/T323 592

0-1

1-2

2-33-44-5Page 140 of 463

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficient ly Random Values	20-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES- CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt. CVE ID : CVE-2023-	ered in Viki before 1.36.x through before 1.38.5, 9.x before CheckUser Manager rely uses AES- cryption with a ed (aka re-used) allowing an ary to decrypt.	
			22912		
Affected Ver	sion(s): From (i	ncluding)	1.36.0 Up to (excluding) 1	.38.5	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	5.4	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time- precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally have the editsitejs capability. CVE ID : CVE-2023-	https://phabr icator.wikime dia.org/T323 592	A-MED- MEDI- 020223/253
Use of Insufficient ly Random Values	20-Jan-2023	5.3	22910 An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser	https://phabr icator.wikime dia.org/T315 123	A-MED- MEDI- 020223/254

0-1

1-2

2-33-44-5Page 141 of 463

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TokenManager insecurely uses AES- CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt.		
			CVE ID : CVE-2023- 22912		
Vendor: Mie	crosoft				
	ge_chromium				
Affected Ver	sion(s): * Up to	(excluding	g) 108.0.1462.95		
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability. CVE ID : CVE-2023- 21775	https://portal .msrc.microso ft.com/en- US/security- guidance/advi sory/CVE- 2023-21775	A-MIC-EDGE- 020223/255
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE- 2023-21795. CVE ID : CVE-2023-	https://portal .msrc.microso ft.com/en- US/security- guidance/advi sory/CVE- 2023-21796	A-MIC-EDGE- 020223/256
Affected Ver	sion(s): * Un to	(excluding	21796 g) 109.0.1518.70		
Allected ver		Cexcluuin		https://portal	
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability. CVE ID : CVE-2023- 21775	.msrc.microso ft.com/en- US/security- guidance/advi sory/CVE- 2023-21775	A-MIC-EDGE- 020223/257
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE- 2023-21796.	https://portal .msrc.microso ft.com/en- US/security- guidance/advi	A-MIC-EDGE- 020223/258

0-1

1-2

2-33-44-5Page 142 of 463

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21795	sory/CVE- 2023-21795	
Incorrect Authorizati on	24-Jan-2023	6.5	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability. CVE ID : CVE-2023- 21719	https://portal .msrc.microso ft.com/en- US/security- guidance/advi sory/CVE- 2023-21719	A-MIC-EDGE- 020223/259
Vendor: mi	niorange				
Product: lda	ap_integration	_with_act	ive_directory_and_openle	dap	
Affected Ver	sion(s): 5.0.2				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	17-Jan-2023	7.5	The 'LDAP Integration with Active Directory and OpenLDAP - NTLM & Kerberos Login' extension is vulnerable to LDAP Injection since is not properly sanitizing the 'username' POST parameter. An attacker can manipulate this paramter to dump arbitrary contents form the LDAP Database. CVE ID : CVE-2023- 23749	N/A	A-MIN-LDAP- 020223/260
Vendor: Mis	sp				
Product: mi	sp				
Affected Ver	sion(s): 2.4.167				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	In MISP 2.4.167, app/webroot/js/action _table.js allows XSS via a network history name. CVE ID : CVE-2023- 24027	https://githu b.com/MISP/ MISP/commit /72c5424034 c378583d128 fc1e769aae33 fb1c8b9	A-MIS-MISP- 020223/261

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID			Pate	:h	NCI	IPC ID	
Vendor: Misp-project										
Product: malware_information_sharing_platform										
Affected Version(s): * Up to (including) 2.4.167										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2023	6.1	uthkey_display.ctp in MISP through 2.4.167 has an XSS in authkey add via a Referer field. CVE ID : CVE-2023-		https:// b.com/M MISP/cc /f7238fe ac065da 8607d02 682f18f	IISP/ mmit e5e71 a43c	A-MIS MALW 02022			
Product: mi	sp									
Affected Ver	sion(s): 2.4.167									
N/A	20-Jan-2023	9.8	app/Contro nent/ACLC hp has inco control for import fun	nent/ACLComponent.p hp has incorrect access control for the decaying import function. CVE ID : CVE-2023-		https:// b.com/M MISP/cc /93bf15 703a326 6cb6c1c 5cf23e3	IISP/ ommit d3bd ebfe8 9b73		-MISP- 3/263	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	app/webro graph.js ha vulnerabili event-grap payload.	CVE ID : CVE-2023-		https:// b.com/M MISP/cc /a46f79 6001101 84fccf3c 983493	IISP/ ommit 4a13 Lcbec		-MISP- 3/264	
Vendor: mo	doboa				1					
Product: mo	odoboa									
Affected Ver	Affected Version(s): * Up to (excluding) 2.0.4									
Cross-Site Request Forgery (CSRF)	19-Jan-2023	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4.			https:// b.com/n oa/mod commit/ ac93669 5fcdebd	nodob oboa/ /8e14 9df4f3	A-MOI MODC 02022		
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	
CV33 SCOTINg S		12 2	J J-4	-+-J	5-0	0-7	7-0	0-5	9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2023- 0398	d2f0fed3ed48 , https://huntr. dev/bounties /0a852351- 00ed-44d2- a650- 9055b7beed5 8			
Cross-Site Request Forgery (CSRF)	23-Jan-2023	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4. CVE ID : CVE-2023- 0438	https://huntr. dev/bounties /07a5b61b- 306d-47c4- 8ff0- 06c540c7dfb3 , https://githu b.com/modob oa/modoboa/ commit/38d7 78cc71e3702 16e067d054c e0169ad8307 8c8	A-MOD- MODO- 020223/266		
Cross-Site Request Forgery (CSRF)	19-Jan-2023	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4. CVE ID : CVE-2023- 0406	https://githu b.com/modob oa/modoboa/ commit/7f05 73e91722768 6d2cc127be1 364e2908740 807, https://huntr. dev/bounties /d7007f76- 3dbc-48a7- a2fb- 377040fe100 c	A-MOD- MODO- 020223/267		
-	Vendor: my_youtube_channel_project						
	Product: my_youtube_channel						
Affected Vers	sion(s): * Up to	(including	g) 3.0.12.1				

0-1

1-2

2-3

3-4 4-5 Page **145** of **463** 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2023	5.5	The My YouTube Channel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its settings parameters in versions up to, and including, 3.0.12.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator- level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID : CVE-2023- 0446	https://plugin s.trac.wordpr ess.org/chang eset?sfp_email =&sfph_mail= &reponame= &old=284420 0%40youtube - channel&new =2844200%4 0youtube- channel&sfp_ email=&sfph_ mail=	A-MYMY_Y- 020223/268
Missing Authorizati on	23-Jan-2023	4.3	The My YouTube Channel plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the clear_all_cache function in versions up to, and including, 3.0.12.1. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to clear the plugin's cache. CVE ID : CVE-2023- 0447	https://plugin s.trac.wordpr ess.org/chang eset?sfp_email =&sfph_mail= &reponame= &old=284420 0%40youtube - channel&new =2844200%4 0youtube- channel&sfp_ email=&sfph_ mail=	A-MYMY_Y- 020223/269
Vendor: Nln	labs				

0-1

1-2

2-3

3-4 4-5 Page **146** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: kr	ill	I		<u> </u>				
Affected Ver	Affected Version(s): * Up to (excluding) 0.12.1							
N/A	17-Jan-2023	7.5	NLnet Labs Krill supports direct access to the RRDP repository content through its built-in web server at the "/rrdp" endpoint. Prior to 0.12.1 a direct query for any existing directory under "/rrdp/", rather than an RRDP file such as "/rrdp/notification.xml " as would be expected, causes Krill to crash. If the built-in "/rrdp" endpoint is exposed directly to the internet, then malicious remote parties can cause the publication server to crash. The repository content is not affected by this, but the availability of the server and repository can cause issues if this attack is persistent and is not mitigated. CVE ID : CVE-2023- 0158	https://www. nlnetlabs.nl/d ownloads/kril l/CVE-2023- 0158.txt	A-NLN-KRIL- 020223/270			
Vendor: oi_y	yandex.maps_j	oroject						
Product: oi	yandex.maps							
Affected Ver	sion(s): * Up to	(including	g) 3.2.7					
Improper Neutralizat ion of Input During Web Page Generation	23-Jan-2023	5.4	Auth. Stored Cross-Site Scripting (XSS) in Oi Yandex.Maps for WordPress <= 3.2.7 versions.	N/A	A-0I0I_Y- 020223/271			
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 147 of 463	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			CVE ID : CVE-2023- 22721		
Vendor: onl	ine_food_orde	ring_syst	em_project	L	
Product: on	line_food_orde	ering_syst	em		
Affected Vers	sion(s): 2.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2023	9.8	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been classified as critical. Affected is an unknown function of the file admin/manage_user.ph p. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB- 218472.	N/A	A-ONL-ONLI- 020223/272
			CVE ID : CVE-2023- 0332		
Vendor: onl	ine_tours_\&_1	ravels_m	anagement_system_proj	ect	
Product: on	line_tours_\&_	travels_n	nanagement_system		
Affected Vers	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2023	9.8	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/page-login.php. The manipulation of the	N/A	A-ONL-ONLI- 020223/273
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-218426 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0324		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	26-Jan-2023	7.2	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This issue affects some unknown processing of the file admin/forget_password .php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-219335. CVE ID : CVE-2023- 0515	N/A	A-ONL-ONLI- 020223/274
Improper Neutralizat ion of Special Elements used in an SQL Command	26-Jan-2023	7.2	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been classified as critical. Affected is an unknown function of the file	N/A	A-ONL-ONLI- 020223/275

0-1

1-2

2-3

3-4 4-5 Page **149** of **463**

-5 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			user/forget_password.p hp of the component Parameter Handler. The manipulation of the argument email leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB- 219336.		
			CVE ID : CVE-2023- 0516		
Vendor: Ora	acle				1
	cess_manager sion(s): 12.2.1.4	ł.0			
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Access Manager executes to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-ACCE- 020223/276

0-1

1-2

2-33-44-5Page 150 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:H/UI:N/S:U/C:H/I:N/ A:N).		
			CVE ID : CVE-2023- 21859		
Product: bi_ Affected Ver	publisher sion(s): 12.2.1.4	4.0			
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:H/I:H/ A:H). CVE ID : CVE-2023- 21832	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BI_P- 020223/277
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher	https://www. oracle.com/se	A-ORA-BI_P- 020223/278

3-4

Page 151 of 463

4-5

5-6

6-7

7-8

8-9

9-10

CVSS Scoring Scale

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:H/I:H/ A:H). CVE ID : CVE-2023- 21846	curity- alerts/cpujan 2023.html	
Affected Ver	sion(s): 5.9.0.0.	0			<u> </u>
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BI_P- 020223/279

0-1

1-2

2-3 3-4 4-5 Page 152 of 463 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:H/I:H/ A:H). CVE ID : CVE-2023- 21832		
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BI_P- 020223/280

0-1

1-2

2-33-44-5Page 153 of 463

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:L/UI:N/S:U/C:H/I:H/ A:H). CVE ID : CVE-2023- 21846		
Affected Ver	<mark>sion(s): 6.4.0.0.</mark>	0			
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:H/I:H/ A:H). CVE ID : CVE-2023- 21832	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BI_P- 020223/281
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BI_P- 020223/282

0-1

1-2

2-33-44-5Page 154 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:H/I:H/ A:H). CVE ID : CVE-2023- 21846		
Product: bu	siness_intellig	ence		I	
Affected Ver	sion(s): 5.9.0.0.	0			
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BUSI- 020223/283

0-1

1-2

2-3

3-4 4-5 Page **155** of **463** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N). CVE ID : CVE-2023- 21861		
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BUSI- 020223/284

0-1

1-2

2-3

5-6

affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise	
exploitable vulnerability allows low privileged attacker with network access via	
vulnerability allows low privileged attacker with network access via	
privileged attacker with network access via	
network access via	
HTTP to compromise	
Oracle Business	
Intelligence Enterprise	
Edition. Successful	
attacks require human	
interaction from a	
person other than the	
attacker and while the	
vulnerability is in	
Oracle Business	
Intelligence Enterprise	
Edition, attacks may	
significantly impact	
additional products	
(scope change).	
Successful attacks of	
this vulnerability can	
result in unauthorized	
update, insert or delete	
access to some of	
Oracle Business	
Intelligence Enterprise	
Edition accessible data	
as well as unauthorized	
read access to a subset	
of Oracle Business	
Intelligence Enterprise	
Edition accessible data.	
CVSS 3.1 Base Score 5.4	
(Confidentiality and	
Integrity impacts).	
CVSS Vector:	
(CVSS:3.1/AV:N/AC:L/P	
R:L/UI:R/S:C/C:L/I:L/A	
:N).	
CVE ID : CVE-2023-	
21891	

0-1

1-2

2-33-44-5Page 157 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.00 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BUSI- 020223/285

0-1

1-2

2-33-44-5Page 158 of 463

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N).		
			CVE ID : CVE-2023- 21892		
Affected Ver	sion(s): 6.4.0.0.	0			
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BUSI- 020223/286

0-1

1-2

2-33-44-5Page 159 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N). CVE ID : CVE-2023- 21861		
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BUSI- 020223/287

0-1

1-2

 2-3
 3-4
 4-5

 Page 160 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N).		
N/A	18-Jan-2023	5.4	21891 Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-BUSI- 020223/288

0-1

1-2

2-33-44-5Page 161 of 463

6-7 7-8

5-6

			Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N). CVE ID : CVE-2023- 21892		
Product: coll	laborative_pla	nning			
			12.2.3 Up to (including)	2.2.12	
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Collaborative Planning product of Oracle E-Business Suite (component:	https://www. oracle.com/se curity-	A-ORA-COLL- 020223/289
CVSS Scoring Sc	cale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 162 of 463	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Installation). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Collaborative Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Collaborative Planning accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21858	alerts/cpujan 2023.html	
Product: co	mmunications.	_billing_a	nd_revenue_managemen	t_elastic_chargi	ng_engine
Affected Ver	sion(s): From (i	ncluding)	12.0.0.3.0 Up to (including	g) 12.0.0.7.0	
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Communications BRM - Elastic Charging Engine product of Oracle Communications Applications (component: Customer, Config, Pricing Manager). Supported versions that are affected are 12.0.0.3.0- 12.0.0.7.0. Easily exploitable vulnerability allows	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- COMM- 020223/290

0-1

1-2

2-3

3-4 4-5 Page **163** of **463** 8-9

9-10

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high privileged attacker with logon to the infrastructure where Oracle Communications BRM - Elastic Charging Engine executes to compromise Oracle Communications BRM - Elastic Charging Engine. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications BRM - Elastic Charging Engine accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:H/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21824		
Product: co	mmunications	_cloud_na	ative_core_binding_suppo	ort_function	
Affected Ver	sion(s): 22.3.0				
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Communications BRM - Elastic Charging Engine product of Oracle Communications Applications (component: Customer, Config, Pricing Manager). Supported versions that are affected are 12.0.0.3.0- 12.0.0.7.0. Easily exploitable vulnerability allows high privileged attacker with logon to the	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- COMM- 020223/291

0-1

1-2

2-33-44-5Page 164 of 463

5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			infrastructure where Oracle Communications BRM - Elastic Charging Engine executes to compromise Oracle Communications BRM - Elastic Charging Engine. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications BRM - Elastic Charging Engine accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:H/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21824		
		_cloud_na	itive_core_policy		
Affected Ver	sion(s): 22.3.0			1	
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Communications BRM - Elastic Charging Engine product of Oracle Communications Applications (component: Customer, Config, Pricing Manager). Supported versions that are affected are 12.0.0.3.0- 12.0.0.7.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Communications	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- COMM- 020223/292

0-1

1-2

2-3

3-4 4-5 Page **165** of **463** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BRM - Elastic Charging Engine executes to compromise Oracle Communications BRM - Elastic Charging Engine. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications BRM - Elastic Charging Engine accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:H/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21824		
Product: co	mmunications	converg	ed_application_server		
	sion(s): 8.0.0	_converg	eu_appneation_seivei		
N/A	18-Jan-2023	9.8	Vulnerability in the Oracle Communications Converged Application Server product of Oracle Communications (component: Core). Supported versions that are affected are 7.1.0 and 8.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via UDP to compromise Oracle Communications Converged Application Server. Successful attacks of this vulnerability can result	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- COMM- 020223/293

0-1

1-2

2-3

3-4 4-5 Page **166** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in takeover of Oracle Communications Converged Application Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:H/ A:H).		
			CVE ID : CVE-2023- 21890		
Affected Ver	sion(s): 7.1.0			I	
N/A	18-Jan-2023	9.8	Vulnerability in the Oracle Communications Converged Application Server product of Oracle Communications (component: Core). Supported versions that are affected are 7.1.0 and 8.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via UDP to compromise Oracle Communications Converged Application Server. Successful attacks of this vulnerability can result in takeover of Oracle Communications Converged Application Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- COMM- 020223/294

0-1

1-2

2-33-44-5Page 167 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:H/ A:H).		
			CVE ID : CVE-2023- 21890		
Product: co	ommunications	_converg	ence		
Affected Ver	rsion(s): 3.0.3.1.	0			
N/A Product: da	18-Jan-2023	8.8	Vulnerability in the Oracle Communications Convergence product of Oracle Communications Applications (component: Admin Configuration). The supported version that is affected is 3.0.3.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Convergence. Successful attacks of this vulnerability can result in takeover of Oracle Communications Convergence. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:H/I:H/ A:H). CVE ID : CVE-2023- 21848	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- COMM- 020223/295
	rsion(s): 19c				

0-1

1-2

2-3

3-4 4-5 Page **168** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	6.3	Vulnerability in the Oracle Database RDBMS Security component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database RDBMS Security. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Database RDBMS Security accessible data as well as unauthorized read access to a subset of Oracle Database RDBMS Security accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:U/C:L/I:H/ A:N). CVE ID : CVE-2023- 21829	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DATA- 020223/296

0-1

1-2

2-33-44-5Page 169 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	4.3	Vulnerability in the Oracle Database Data Redaction component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database Data Redaction. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Database Data Redaction accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:L/I:N/ A:N). CVE ID : CVE-2023- 21827	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DATA- 020223/297
Affected Ver	sion(s): 21c				
N/A	18-Jan-2023	6.3	Vulnerability in the Oracle Database RDBMS Security component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DATA- 020223/298

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with network access via Oracle Net to compromise Oracle Database RDBMS Security. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Database RDBMS Security accessible data as well as unauthorized read access to a subset of Oracle Database RDBMS Security accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:U/C:L/I:H/ A:N). CVE ID : CVE-2023- 21829		
N/A	18-Jan-2023	4.3	Vulnerability in the Oracle Database Data Redaction component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DATA- 020223/299

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with network access via Oracle Net to compromise Oracle Database Data Redaction. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Database Data Redaction accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:L/I:N/ A:N). CVE ID : CVE-2023-		
Product: da	tabase_server		21827		
Affected Ver					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Data Provider for .NET component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TCPS to compromise Oracle Data Provider for .NET. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DATA- 020223/300

0-1

1-2

2-33-44-5Page 172 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Data Provider for .NET. Note: Applies also to Database client-only on Windows platform. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:R/S:U/C:H/I:H /A:H). CVE ID : CVE-2023- 21893		
Affected Ver	sion(s): 21c		<u> </u>	l	
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Data Provider for .NET component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TCPS to compromise Oracle Data Provider for .NET. Successful attacks require human interaction from a person other than the attacker. Successful attacker. Successful attacks of this vulnerability can result in takeover of Oracle Data Provider for .NET. Note: Applies also to Database client-only on Windows platform. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DATA- 020223/301

0-1

1-2

2-33-44-5Page 173 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:R/S:U/C:H/I:H /A:H).					
			CVE ID : CVE-2023- 21893					
Product: de	emantra_demai	ıd_manaş	gement					
Affected Version(s): 12.1								
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Demantra Demand Management product of Oracle Supply Chain (component: E- Business Collections). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Demantra Demand Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DEMA- 020223/302			

0-1

1-2

2-33-44-5Page 174 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21850		
Affected Vers	sion(s): 12.2			I	1
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Demantra Demand Management product of Oracle Supply Chain (component: E- Business Collections). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Demantra Demand Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21850	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- DEMA- 020223/303
	sion(s): From (i	ncluding)	12.2.3 Up to (including) 1	2.2.12	
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Applications	https://www. oracle.com/se	A-ORA-E-BU- 020223/304
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 175 of 463	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DBA product of Oracle E-Business Suite (component: Java utils). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications DBA accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21849	curity- alerts/cpujan 2023.html	
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Download). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-E-BU- 020223/305

0-1

1-2

2-3

5-6

6-7

HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, attacks may							
significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web Applications Desktop Integrator accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N).							
CVE ID : CVE-2023- 21847							
Product: global_lifecycle_management_nextgen_oui_framework							
Affected Version(s): * Up to (excluding) 13.9.4.2.11	Affected Vers						

0-1

1-2

3-4 4-5 2-3

7-8 8-9

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	7.3	Vulnerability in the Oracle Global Lifecycle Management NextGen OUI Framework product of Oracle Fusion Middleware (component: NextGen Installer issues). Supported versions that are affected are Prior to 13.9.4.2.11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Global Lifecycle Management NextGen OUI Framework executes to compromise Oracle Global Lifecycle Management NextGen OUI Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Global Lifecycle Management NextGen OUI Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Global Lifecycle Management NextGen OUI Framework. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:R/S:U/C:H/I:H/ A:H).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GLOB- 020223/306

0-1

1-2

2-33-44-5Page 178 of 463

7-8 8-9 9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 21894							
Product: gr	Product: graalvm									
Affected Ver	sion(s): 22.3.0									
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g.,	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/307					

0-1

1-2

2-3

3-4 4-5 Page **179** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/308

0-1

1-2

2-33-44-5Page 180 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:L). CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5,	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/309

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.0.1; Oracle GraalVM		
			Enterprise Edition:		
			20.3.8, 21.3.4 and		
			22.3.0. Difficult to		
			exploit vulnerability		
			allows unauthenticated		
			attacker with network		
			access via multiple		
			protocols to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			update, insert or delete		
			access to some of		
			Oracle Java SE, Oracle		
			GraalVM Enterprise		
			Edition accessible data.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 3.7		
			(Integrity impacts).		
			CVSS Vector:		
			(CVSS:3.1/AV:N/AC:H/		

0-1

1-2

2-33-44-5Page 182 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023- 21843		
Affected Ver	sion(s): 20.3.8				
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/310

0-1

1-2

2-33-44-5Page 183 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023-		
N/A	18-Jan-2023	5.3	21830 Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/311

0-1

1-2

2-33-44-5Page 184 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:L). CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/312

0-1

1-2

2-3

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perf, 11.0.17, 17.0.5,		
			19.0.1; Oracle GraalVM		
			Enterprise Edition:		
			20.3.8, 21.3.4 and		
			22.3.0. Difficult to		
			exploit vulnerability		
			allows unauthenticated		
			attacker with network		
			access via multiple		
			protocols to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			update, insert or delete		
			access to some of		
			Oracle Java SE, Oracle		
			GraalVM Enterprise		
			Edition accessible data.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 3.7		
			(Integrity impacts).		
			CVSS Vector:		

0-1

1-2

2-33-44-5Page 186 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			(CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023- 21843							
Affected Ver	Affected Version(s): 21.3.4									
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Applets,	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/313					

0-1

1-2

2-3

3-4 4-5 Page **187** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/314

0-1

1-2

2-33-44-5Page 188 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:L). CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- GRAA- 020223/315

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE: 8u351, 8u351-		
			perf, 11.0.17, 17.0.5,		
			19.0.1; Oracle GraalVM		
			Enterprise Edition:		
			20.3.8, 21.3.4 and		
			22.3.0. Difficult to		
			exploit vulnerability		
			allows unauthenticated		
			attacker with network		
			access via multiple		
			protocols to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			update, insert or delete		
			access to some of		
			Oracle Java SE, Oracle		
			GraalVM Enterprise		
			Edition accessible data.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 3.7		
			(Integrity impacts).		

0-1

1-2

2-33-44-5Page 190 of 463

6-7 7-8

5-6

N/A 18-Jan-2023 7.5 7.5 Architecture. Successful attacks of critical data or all Oracle HCM Common Architecture. https://www. oracle.com/se A-ORA- HCM UINTP to compromise Oracle Component: Auomated Test Suite). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle MCM Common Architecture. https://www. Oracle.com/se curity- alerts/cpujan 2023.html A-ORA- HCM UINTP to compromise Oracle VULNESULT Component: Auomated Test Suite). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle VINTP to compromise Oracle VINTP to compromise Oracle vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC.L/P R:M/ULN/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21857 A-ORA- HCM 020223/316	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: hcm_common_architecture Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12 Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12 Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Auomated Test Suite). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 Jase Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UEN/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21857 A-ORA- HCM 020223/316				(CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023-						
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12 Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Auomated Test Suite). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 JAV:N/AC:L/P R:N/U:N/S:U/C:N/I:H/ A:N). A-ORA- HCM 020223/316 Product: hospitality_reporting_and_analytics CVE ID : CVE-2023- 21857 It is unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 JAV:N/AC:L/P R:N/U:N/S:U/C:N/I:H/ A:N). It is unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 JAV:N/AC:L/P R:N/U:N/S:U/C:N/I:H/ A:N).	Des des et la		-1-144							
N/A18-Jan-20237.5Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Auomated Test Suite). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture.https://www. A-ORA- HCM- 02023/316N/A18-Jan-20237.57.5Architecture. Compromise Oracle HCM Common Architecture.https://www. oracle.com/se curity- alerts/cpujan 2023.htmlA-ORA- HCM- 020223/316N/A18-Jan-20237.5Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS: 3.1/AV:N/AC:L/P R:N/U:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21857Product: hospitality_reporting_and_analytics										
	N/A			Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Auomated Test Suite). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023-	https://www. oracle.com/se curity- alerts/cpujan	HCM				
	Product: ho	spitality_repo	rting_and	_analytics	I					
			1 2							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.1.0	•			
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:H/I:H/ A:N). CVE ID : CVE-2023- 21828	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- HOSP- 020223/317

0-1

1-2

2-33-44-5Page 192 of 463

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	7.6	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker. Successful attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Reporting and Analytics. CVSS 3.1 Base Score 7.6	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- HOSP- 020223/318

0-1

1-2

2-33-44-5Page 193 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:U/C:H/I:L/ A:H).		
			CVE ID : CVE-2023- 21826		
Product: ise	etup				
Affected Ver	sion(s): From (i	ncluding)	12.2.3 Up to (including) 12	2.2.12	
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSetup accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21856	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-ISET- 020223/319

0-1

1-2

2-33-44-5Page 194 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: isu	ipplier_portal	I	L	L	L
Affected Ver	sion(s): From (i	ncluding)	12.2.6 Up to (including) 12	2.2.8	
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle iSupplier Portal product of Oracle E- Business Suite (component: Supplier Management). Supported versions that are affected are 12.2.6- 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iSupplier Portal accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:L/I:N/ A:N). CVE ID : CVE-2023- 21825	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-ISUP- 020223/320
Product: jdl	K				
Affected Ver	sion(s): 1.8.0				
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/321

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected are Oracle		
			Java SE: 8u351, 8u351-		
			perf; Oracle GraalVM		
			Enterprise Edition:		
			20.3.8 and 21.3.4.		
			Easily exploitable		
			vulnerability allows		
			unauthenticated		
			attacker with network		
			access via multiple		
			protocols to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			update, insert or delete		
			access to some of		
			Oracle Java SE, Oracle		
			GraalVM Enterprise		
			Edition accessible data.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 5.3		
			(Integrity impacts).		

0-1

1-2

2-3

3-4 4-5 Page **196** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/322

0-1

1-2

2-3

3-4 4-5 Page **197** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023- 21843		
Affected Ver	sion(s): 11.0.17				
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/323

0-1

1-2

2-3

3-4 4-5 Page **198** of **463** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/324

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that		
			are affected are Oracle		
			Java SE: 11.0.17, 17.0.5,		
			19.0.1; Oracle GraalVM		
			Enterprise Edition:		
			20.3.8, 21.3.4 and		
			22.3.0. Easily		
			exploitable		
			vulnerability allows		
			unauthenticated		
			attacker with network		
			access via DTLS to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			ability to cause a partial		
			denial of service		
			(partial DOS) of Oracle		
			Java SE, Oracle GraalVM		
			Enterprise Edition.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 5.3		

0-1

1-2

2-33-44-5Page 200 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:L).		
			CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/325

0-1

1-2

2-33-44-5Page 201 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023- 21843		
Affected Ver	sion(s): 17.0.5				
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/326

0-1

1-2

 2-3
 3-4
 4-5

 Page 202 of 463

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830	https://www.	
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/327

0-1

1-2

5-6

6-7

7-8

2-3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: JSSE).		
			Supported versions that		
			are affected are Oracle		
			Java SE: 11.0.17, 17.0.5,		
			19.0.1; Oracle GraalVM		
			Enterprise Edition:		
			20.3.8, 21.3.4 and		
			22.3.0. Easily		
			exploitable		
			vulnerability allows		
			unauthenticated		
			attacker with network		
			access via DTLS to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			ability to cause a partial		
			denial of service		
			(partial DOS) of Oracle		
			Java SE, Oracle GraalVM		
			Enterprise Edition.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		

0-1

1-2

 2-3
 3-4
 4-5

 Page 204 of 463

6-7

7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:L).		
			CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/328

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023-		
Affected Ver	sion(s): 19.0.1		21843		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/329

0-1

1-2

 2-3
 3-4
 4-5

 Page
 206 of
 463

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www. oracle.com/se curity-	A-ORA-JDK- 020223/330

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE	alerts/cpujan	
			(component: JSSE).	2023.html	
			Supported versions that		
			are affected are Oracle		
			Java SE: 11.0.17, 17.0.5,		
			19.0.1; Oracle GraalVM		
			Enterprise Edition:		
			20.3.8, 21.3.4 and		
			22.3.0. Easily		
			exploitable		
			vulnerability allows		
			unauthenticated		
			attacker with network		
			access via DTLS to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			ability to cause a partial		
			denial of service		
			(partial DOS) of Oracle Java SE, Oracle GraalVM		
			Enterprise Edition.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		

0-1

1-2

2-3

6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:L).		
			CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JDK- 020223/331

0-1

1-2

2-3

3-4 4-5 Page **209** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023- 21843		
Product: jre	sion(s): 1.8.0				
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/332

0-1

1-2

2-3

3-4 4-5 Page **210** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle	https://www. oracle.com/se	A-ORA-JRE- 020223/333

0-1

1-2

2-33-44-5Page 211 of 463

5-6

6-7

8-9

GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 80351, 80351, 80351, Perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in cacessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not
apply to Java deployments, typically

0-1

1-2

2-3 3-4 4-5 Page **212** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023- 21843		
Affected Ver	sion(s): 11.0.17			1	<u> </u>
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data.	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/334

0-1

1-2

2-3 3-4 4-5 Page 213 of 463 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023-		
N/A	18-Jan-2023	5.3	21830 Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/335

0-1

1-2

2-33-44-5Page 214 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated		
			attacker with network		
			access via DTLS to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			ability to cause a partial		
			denial of service		
			(partial DOS) of Oracle		
			Java SE, Oracle GraalVM		
			Enterprise Edition.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 5.3		
			(Availability impacts).		
			CVSS Vector:		
			(CVSS:3.1/AV:N/AC:L/P		
			R:N/UI:N/S:U/C:N/I:N/		
			A:L).		
			CVE ID : CVE-2023-		
			21835		

0-1

1-2

2-3 3-4 4-5 Page 215 of 463 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/336

0-1

1-2

2-3

3-4 4-5 Page **216** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N). CVE ID : CVE-2023- 21843		
Affected Ver	sion(s): 17.0.5			I	1
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/337

0-1

1-2

2-3

3-4 4-5 Page **217** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/338

0-1

1-2

2-33-44-5Page 218 of 463

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable		
			vulnerability allows		
			unauthenticated		
			attacker with network		
			access via DTLS to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			ability to cause a partial		
			denial of service		
			(partial DOS) of Oracle		
			Java SE, Oracle GraalVM		
			Enterprise Edition.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 5.3		
			(Availability impacts).		
			CVSS Vector:		
			(CVSS:3.1/AV:N/AC:L/P		
			R:N/UI:N/S:U/C:N/I:N/		
			A:L).		

0-1

1-2

2-3 3-4 4-5 Page 219 of 463 5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/339

0-1

1-2

2-3

3-4 4-5 Page **220** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N).		
			CVE ID : CVE-2023- 21843		
Affected Ver	sion(s): 19.0.1				
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/340

0-1

1-2

2-3 3-4 4-5 Page **221** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21830		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition:	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/341

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.8, 21.3.4 and		
			22.3.0. Easily		
			exploitable		
			vulnerability allows		
			unauthenticated		
			attacker with network		
			access via DTLS to		
			compromise Oracle Java		
			SE, Oracle GraalVM		
			Enterprise Edition.		
			Successful attacks of		
			this vulnerability can		
			result in unauthorized		
			ability to cause a partial		
			denial of service		
			(partial DOS) of Oracle		
			Java SE, Oracle GraalVM		
			Enterprise Edition.		
			Note: This vulnerability		
			applies to Java		
			deployments, typically		
			in clients running		
			sandboxed Java Web		
			Start applications or		
			sandboxed Java applets,		
			that load and run		
			untrusted code (e.g.,		
			code that comes from		
			the internet) and rely		
			on the Java sandbox for		
			security. This		
			vulnerability does not		
			apply to Java		
			deployments, typically		
			in servers, that load and		
			run only trusted code		
			(e.g., code installed by		
			an administrator). CVSS		
			3.1 Base Score 5.3		
			(Availability impacts).		
			CVSS Vector:		
			(CVSS:3.1/AV:N/AC:L/P		
			R:N/UI:N/S:U/C:N/I:N/		
			A:L).		

0-1

1-2

2-3 3-4 4-5 Page 223 of 463 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351- perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-JRE- 020223/342

0-1

1-2

2-3

3-4 4-5 Page **224** of **463** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:N/I:L /A:N).		
			CVE ID : CVE-2023- 21843		
	arning_manage				
Affected Ver	sion(s): From (i	ncluding)	12.2.3 Up to (including) 12	2.2.12	Γ
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Learning Management product of Oracle E-Business Suite (component: Setup). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Learning Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Learning Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-LEAR- 020223/343

0-1

1-2

2-3

3-44-5Page 225 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023-			
			21852			
Product: ma	U	1 1: >		2.2.4.2		
Affected Vers	sion(s): From (i	ncluding)		2.2.12		
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12 Vulnerability in the Oracle Marketing product of Oracle E- Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacks of this vulnerability can result in unauthorized creation access to critical data or all Oracle Marketing accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). https://www. oracle.com/se curity- alerts/cpujan 2023/344						
Product: mo	bile_field_serv	vice				

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12							
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Mobile Field Service product of Oracle E-Business Suite (component: Synchronization). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Mobile Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Mobile Field Service accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21853	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MOBI- 020223/345			
Product: my	ysql			I				
Affected Ver	sion(s): From (i	ncluding)	8.0 Up to (including) 8.0.3	1				
N/A	18-Jan-2023	5.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.31	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/346			

0-1

1-2

 2-3
 3-4
 4-5

 Page 227 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:H/UI:N/S:U/C:N/I:H /A:H). CVE ID : CVE-2023- 21875		
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/347

0-1

1-2

2-33-44-5Page 228 of 463

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:L/ A:H). CVE ID : CVE-2023- 21877		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/348

0-1

1-2

2-3

3-4 4-5 Page **229** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H).		
			CVE ID : CVE-2023- 21876		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21878	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/349
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/350

0-1

1-2

2-3

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023-		
Affected Ver	sion(s): From (i	ncluding)	21879 8.0.0 Up to (including) 8.0	.31	
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/351

0-1

1-2

2-3

3-4 4-5 Page **231** of **463** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:L/ A:H). CVE ID : CVE-2023-		
N/A	18-Jan-2023	4.9	21880 Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/352

0-1

1-2

 2-3
 3-4
 4-5

 Page
 232
 of
 463

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21881		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21883	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/353
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/354

0-1

1-2

2-3

3-4 4-5 Page **233** of **463** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023-		
N/A	18-Jan-2023	2.7	21887 Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/355

0-1

1-2

2-33-44-5Page234 of463

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			R:H/UI:N/S:U/C:N/I:L/ A:N).						
			CVE ID : CVE-2023- 21882						
Product: my	Product: mysql_cluster								
Affected Ver	sion(s): From (i	ncluding)	8.0.0 Up to (including) 8.0	.31					
N/A	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/356				

0-1

1-2

2-33-44-5Page 235 of 463

5-6

6-7

 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PR:H/UI:R/S:U/C:H/I:H /A:H). CVE ID : CVE-2023- 21860		
Affected Ver	sion(s): From (i	ncluding)	7.4.0 Up to (including) 7.4	.38	
N/A	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/ PR:H/UI:R/S:U/C:H/I:H /A:H).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/357

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21860		
Affected Ver	sion(s): From (i	ncluding)	7.5.0 Up to (including) 7.5	.28	
N/A	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/ PR:H/UI:R/S:U/C:H/I:H /A:H). CVE ID : CVE-2023- 21860	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/358

0-1

1-2

2-33-44-5Page 237 of 463

6-7 7-8

5-6

Affected Vers			Description & CVE ID		NCIIPC ID		
Affected Version(s): From (including) 7.6.0 Up to (including) 7.6.24							
N/A Product: my	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/ PR:H/UI:R/S:U/C:H/I:H /A:H). CVE ID : CVE-2023- 21860	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/359		
•	•	ncluding)	8.0.0 Up to (including) 8.0	.31			

0-1

1-2

2-3

3-4 4-5 Page **238** of **463** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21868	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/360
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/361

0-1

1-2

2-3

3-4 4-5 Page **239** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:L/ A:H). CVE ID : CVE-2023- 21869		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/362

0-1

1-2

 2-3
 3-4
 4-5

 Page
 240 of
 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H).		
			CVE ID : CVE-2023- 21836		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21863	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/363
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/364

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21867		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/365

0-1

1-2

2-3

3-4 4-5 Page **242** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H).		
			CVE ID : CVE-2023- 21870		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21871	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/366
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/367

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023-		
Affected Ver	sion(s): From (i	ncluding)	21873 5.7.0 Up to (including) 5.7	/.40	
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.40 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/368

0-1

1-2

2-3

3-4 4-5 Page **244** of **463** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H).		
			CVE ID : CVE-2023- 21840		
Affected Vers	sion(s): From (i	ncluding)	8.0.0 Up to (including) 8.0	.28	
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21866	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/369
Affected Vers	sion(s): From (i	ncluding)	8.0.0 Up to (including) 8.0	.29	

0-1

1-2

3-4 4-5 2-3

8-9 7-8 9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:L/ A:H). CVE ID : CVE-2023- 21872	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/370
Affected Ver	sion(s): From (i	ncluding)	8.0.0 Up to (including) 8.0	.30	
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/371

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21864		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/372

0-1

1-2

2-3

3-4 4-5 Page **247** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023-			
			21865			
N/A	18-Jan-2023	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:L). CVE ID : CVE-2023- 21874	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- MYSQ- 020223/373	
Product: pe Affected Ver	•	prise_cs_a	academic_advisement			
N/A	18-Jan-2023	5.3	Vulnerability in the PeopleSoft Enterprise CS Academic	https://www. oracle.com/se curity-	A-ORA-PEOP- 020223/374	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 248 G 463						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Advisement product of Oracle PeopleSoft (component: Advising Notes). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Academic Advisement. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Academic Advisement accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:L/I:N/ A:N). CVE ID : CVE-2023- 21831	alerts/cpujan 2023.html	
Product: pe	oplesoft_enter	prise_peo	opletools		
Affected Ver	sion(s): 8.59				
N/A	18-Jan-2023	5.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with network access via	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-PEOP- 020223/375

0-1

1-2

2-33-44-5Page 249 of 463

8-9

9-10

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N). CVE ID : CVE-2023- 21844		
Affected Ver	sion(s): 8.60			l	
N/A	18-Jan-2023	5.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-PEOP- 020223/376

1-2

5-6

6-7

versions that are affected are 8.59 and	
affected are 8.59 and	
8.60. Easily exploitable	
vulnerability allows low	
privileged attacker with	
network access via	
HTTP to compromise	
PeopleSoft Enterprise	
PeopleTools. Successful	
attacks require human	
interaction from a	
person other than the	
attacker and while the	
vulnerability is in	
PeopleSoft Enterprise	
PeopleTools, attacks	
may significantly	
impact additional	
products (scope	
change). Successful	
attacks of this	
vulnerability can result	
in unauthorized	
update, insert or delete	
access to some of	
PeopleSoft Enterprise	
PeopleTools accessible	
data as well as	
unauthorized read	
access to a subset of	
PeopleSoft Enterprise	
PeopleTools accessible	
data. CVSS 3.1 Base	
Score 5.4	
(Confidentiality and	
Integrity impacts).	
CVSS Vector:	
(CVSS:3.1/AV:N/AC:L/P	
R:L/UI:R/S:C/C:L/I:L/A	
:N).	
CVE ID : CVE-2023-	
21844	

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	5.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Panel Processor). The supported version that is affected is 8.60. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:L/I:L/A :N). CVE ID : CVE-2023- 21845	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-PEOP- 020223/377
-	imavera_gatev sion(s): From (i	-	18.8.0 Up to (including) 1	8.8.15	
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and	https://www. oracle.com/se curity-	A-ORA-PRIM- 020223/378
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 252 of 463	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID Engineering (component: WebUI). Supported versions that are affected are 18.8.0- 18.8.15, 19.12.0- 19.12.15, 20.12.0- 20.12.10 and 21.12.0- 21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may	Patch alerts/cpujan 2023.html	NCIIPC ID
			accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N).		

0-1

1-2

2-33-44-5Page 253 of 463

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21888		
Affected Ver	sion(s): From (i	ncluding)	19.12.0 Up to (including)	19.12.15	
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and Engineering (component: WebUI). Supported versions that are affected are 18.8.0- 18.8.15, 19.12.0- 19.12.15, 20.12.0- 20.12.10 and 21.12.0- 21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-PRIM- 020223/379

0-1

1-2

2-33-44-5Page 254 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N).		
			CVE ID : CVE-2023- 21888		
Affected Ver	rsion(s): From (i	ncluding)	20.12.0 Up to (including)	20.12.10	
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and Engineering (component: WebUI). Supported versions that are affected are 18.8.0- 18.8.15, 19.12.0- 19.12.15, 20.12.0- 20.12.10 and 21.12.0- 21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-PRIM- 020223/380

0-1

1-2

2-33-44-5Page 255 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N).		
			CVE ID : CVE-2023- 21888		
Affected Ver	sion(s): From (i	ncluding)	21.12.0 Up to (including)	21.12.8	
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and Engineering (component: WebUI). Supported versions that are affected are 18.8.0- 18.8.15, 19.12.0- 19.12.15, 20.12.0- 20.12.10 and 21.12.0- 21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-PRIM- 020223/381

0-1

1-2

2-33-44-5Page256 of463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:R/S:C/C:L/I:L/A :N). CVE ID : CVE-2023- 21888		
	les_for_handhe				
Affected Ver	sion(s): From (i	ncluding)	12.2.3 Up to (including) 12	2.2.12	
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Sales for Handhelds product of Oracle E-Business Suite (component: Pocket Outlook Sync(PocketPC)). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales for Handhelds. Successful attacks of	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-SALE- 020223/382

0-1

1-2

2-3

3-4 4-5 Page **257** of **463** 5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales for Handhelds accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21855		
Product: sa	les_offline				
Affected Ver	sion(s): From (i	ncluding)	12.2.3 Up to (including) 12	2.2.12	
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Sales Offline product of Oracle E- Business Suite (component: Core Components). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales Offline accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-SALE- 020223/383

0-1

1-2

2-33-44-5Page 258 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:H/ A:N). CVE ID : CVE-2023- 21854		
Product: se	lf-service_hum	an rasou			
			12.2.3 Up to (including) 12	2.2.12	
N/A	18-Jan-2023	4.3	Vulnerability in the Oracle Self-Service Human Resources product of Oracle E- Business Suite (component: Workflow, Approval, Work Force Management). Supported versions that are affected are 12.2.3- 12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Self-Service Human Resources. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Self-Service Human Resources accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:L/UI:N/S:U/C:N/I:L/ A:N). CVE ID : CVE-2023- 21834	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-SELF- 020223/384

0-1

1-2

2-33-44-5Page 259 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: vn	n_virtualbox			I	1			
Affected Version(s): * Up to (excluding) 6.1.42								
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:H/I:H /A:H). CVE ID : CVE-2023- 21886	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/385			
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/386			

0-1

1-2

 2-3
 3-4
 4-5

 Page 260 of 463

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21898		
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/387

0-1

1-2

2-33-44-5Page 261 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21899		
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/388

0-1

1-2

 2-3
 3-4
 4-5

 Page 262 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H).		
			CVE ID : CVE-2023- 21884		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Applies to Windows only. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/389

0-1

1-2

2-33-44-5Page 263 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:L/UI:N/S:C/C:L/I:N/ A:N). CVE ID : CVE-2023- 21885		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:N/S:C/C:L/I:N/ A:N). CVE ID : CVE-2023- 21889	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/390
Affected Ver	sion(s): From (i	ncluding)	7.0.0 Up to (excluding) 7.0	0.6	

0-1

1-2

 2-3
 3-4
 4-5

 Page 264 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:N/UI:N/S:U/C:H/I:H /A:H). CVE ID : CVE-2023- 21886	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/391
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/392

0-1

1-2

2-3

3-4 4-5 Page **265** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21898		
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/393

0-1

1-2

2-33-44-5Page 266 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023-		
			21899		
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/394

0-1

1-2

 2-3
 3-4
 4-5

 Page 267 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:H/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21884		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Applies to Windows only. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:N/S:C/C:L/I:N/ A:N).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/395

0-1

1-2

2-33-44-5Page 268 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21885		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P R:L/UI:N/S:C/C:L/I:N/ A:N). CVE ID : CVE-2023- 21889	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA-VM_V- 020223/396
Product: we	eblogic_server				
Affected Ver	sion(s): 12.2.1.4	ł.0			

0-1

1-2

2-33-44-5Page 269 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21837	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/397
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/398

0-1

1-2

2-3

3-4 4-5 Page **270** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023-		
N/A	18-Jan-2023	7.5	21838 Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/399

0-1

1-2

2-33-44-5Page 271 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N).		
			CVE ID : CVE-2023- 21839		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21841	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/400
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware	https://www. oracle.com/se curity-	A-ORA- WEBL- 020223/401

0-1

1-2

2-3 3-4 4-5 Page 272 of 463 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21842	alerts/cpujan 2023.html	
Affected Ver	sion(s): 12.2.1.3	3.0	L	I	
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/402

0-1

1-2

2-33-44-5Page 273 of 463

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023-		
N/A	18-Jan-2023	7.5	21837 Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/403

0-1

1-2

2-33-44-5Page 274 of 463

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023-		
			21838		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21839	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/404
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/405

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21841		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/406

0-1

1-2

2-33-44-5Page 276 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21842		
Affected Ver	sion(s): 14.1.1.).0	<u> </u>		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/407

0-1

1-2

2-33-44-5Page 277 of 463

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:N/UI:N/S:U/C:H/I:N/ A:N).		
			CVE ID : CVE-2023- 21837		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:N/I:N/ A:H). CVE ID : CVE-2023- 21838	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/408
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/409

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21839		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/410

0-1

1-2

2-33-44-5Page 279 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N). CVE ID : CVE-2023- 21841		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:N/S:U/C:H/I:N/ A:N).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEBL- 020223/411

0-1

1-2

 2-3
 3-4
 4-5

 Page 280 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21842		
Product: we	eb_services_ma	nager			
Affected Ver	rsion(s): 12.2.1.4	ł.0			
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware (component: XML Security component). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Services Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Services Manager accessible data as well as unauthorized access to acritical data or complete access to all Oracle Web Services Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and	https://www. oracle.com/se curity- alerts/cpujan 2023.html	A-ORA- WEB 020223/412

0-1

1-2

2-33-44-5Page 281 of 463

6-7 7-8

5-6

			Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P R:N/UI:R/S:U/C:H/I:H/ A:N). CVE ID : CVE-2023-		
			21862		
Vendor: ora	-				
Product: ora	0				
Affected Vers	sion(s): 2.0.11				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injoction')	18-Jan-2023	8.8	OrangeScrum version 2.0.11 allows an authenticated external attacker to execute arbitrary commands on the server. This is possible because the application injects an attacker-controlled parameter into a system function.	N/A	A-ORA- ORAN- 020223/413
Injection')			CVE ID : CVE-2023- 0164		
Vendor: pga					
Product: pga		ncluding	4.0 Up to (excluding) 6.14		
Allected vers		liciuuliigj			
URL Redirectio n to Untrusted Site ('Open Redirect')	17-Jan-2023	6.1	Open redirect vulnerability in pgAdmin 4 versions prior to v6.14 allows a remote unauthenticated attacker to redirect a user to an arbitrary web site and conduct a phishing attack by having a user to access a specially crafted URL. CVE ID : CVE-2023- 22298	https://githu b.com/pgadm in- org/pgadmin 4/issues/534 3, https://www. pgadmin.org/	A-PGA-PGAD- 020223/414
Vendor: Pim	ncore			l	l
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pin	mcore	I			I
Affected Ver	sion(s): * Up to	(excluding	g) 10.5.14		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.14. CVE ID : CVE-2023- 0323	https://huntr. dev/bounties /129d6a4b- 0504-4de1- a72c- 3f12c455234 3, https://githu b.com/pimcor e/pimcore/co mmit/746fac 1a342841624 f63ab13edcd3 40358e1bc04	A-PIM-PIMC- 020223/415
Vendor: pkg	gconf				
Product: pk	gconf				
Affected Ver	sion(s): * Up to	(including	g) 1.9.3		
N/A	22-Jan-2023	9.8	In pkgconf through 1.9.3, variable duplication can cause unbounded string expansion due to incorrect checks in libpkgconf/tuple.c:pkgc onf_tuple_parse. For example, a .pc file containing a few hundred bytes can expand to one billion bytes. CVE ID : CVE-2023- 24056	https://gitea.t reehouse.syst ems/ariadne/ pkgconf/com mit/628b2b2 bafa5d3a201 7193ddf3750 93e70666059	A-PKG-PKGC- 020223/416
Vendor: Ple	sk				
Product: ob	sidian				
Affected Ver	sion(s): * Up to	(including	g) 18.0.49		
URL Redirectio n to	22-Jan-2023	6.1	A Host Header Injection issue on the Login page of Plesk Obsidian	N/A	A-PLE-OBSI- 020223/417

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4
 4-5
 5-6
 6-7
 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			through 18.0.49 allows attackers to redirect users to malicious websites via a Host request header.		
			CVE ID : CVE-2023- 24044		
Vendor: Pov	werdns				
Product: re	cursor				
Affected Ver	sion(s): 4.8.0	-		-	
Uncontroll ed Recursion	21-Jan-2023	7.5	A remote attacker might be able to cause infinite recursion in PowerDNS Recursor 4.8.0 via a DNS query that retrieves DS records for a misconfigured domain, because QName minimization is used in QM fallback mode. This is fixed in 4.8.1. CVE ID : CVE-2023- 22617	https://docs.p owerdns.com /recursor/cha ngelog/4.8.ht ml#change- 4.8.1, https://docs.p owerdns.com /recursor/sec urity- advisories/	A-POW- RECU- 020223/418
Vendor: pyl	oad				
Product: py					
Affected Ver	sion(s): * Up to	(including	g) 0.4.20		
N/A	22-Jan-2023	9.8	Excessive Attack Surface in GitHub repository pyload/pyload prior to 0.5.0b3.dev41. CVE ID : CVE-2023- 0435	https://huntr. dev/bounties /a3e32ad5- caee-4f43- b10a- 4a876d4e3f1 d, https://githu b.com/pyload /pyload/com mit/431ea6f0 371d748df66	A-PYL-PYLO- 020223/419

0-1

1-2

 2-3
 3-4
 4-5

 Page 284 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b344a05ca1a	
				8e0310cff3	
Affected Ver	sion(s): * Up to	(including	g) 0.4.9		
Improper Input Validation	22-Jan-2023	7.5	Improper Input Validation in GitHub repository pyload/pyload prior to 0.5.0b3.dev40. CVE ID : CVE-2023- 0434	https://githu b.com/pyload /pyload/com mit/a2b1eb1 028f45ac58de a5f58593c1d 3db2b4a104, https://huntr. dev/bounties /7d9332d8- 6997-483b- 9fb9- bcf2ae01dad4	A-PYL-PYLO- 020223/420
Affected Ver	sion(s): 0.5.0				
Improper Input Validation	22-Jan-2023	7.5	Improper Input Validation in GitHub repository pyload/pyload prior to 0.5.0b3.dev40. CVE ID : CVE-2023- 0434	https://githu b.com/pyload /pyload/com mit/a2b1eb1 028f45ac58de a5f58593c1d 3db2b4a104, https://huntr. dev/bounties /7d9332d8- 6997-483b- 9fb9- bcf2ae01dad4	A-PYL-PYLO- 020223/421
Vendor: Raj					
Product: ve	<u> </u>				
Affected Ver	sion(s): * Up to	(excluding	g) 0.6.7-5		
Missing Authorizati on	18-Jan-2023	8.8	Rapid7 Velociraptor allows users to be created with different privileges on the server. Administrators are generally allowed to run any command on the server including	https://docs.v elociraptor.ap p/announcem ents/2023- cves/#:~:text =to%20upgra de%20clients. -	A-RAP-VELO- 020223/422

0-1

1-2

 2-3
 3-4
 4-5

 Page 285 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			writing arbitrary files.	,CVE%2D202	
			However, lower	3%2D0242,-	
			privilege users are	Insufficient%	
			generally forbidden	20Permission	
			from writing or	%20Check	
			modifying files on the		
			server. The VQL copy()		
			function applies		
			permission checks for		
			reading files but does		
			not check for		
			permission to write		
			files. This allows a low		
			privilege user (usually,		
			users with the		
			Velociraptor		
			"investigator" role) to		
			overwrite files on the		
			server, including		
			Velociraptor		
			configuration files. To		
			exploit this		
			vulnerability, the		
			attacker must already		
			have a Velociraptor user account at a low		
			privilege level (at least		
			"analyst") and be able		
			to log into the GUI and		
			create a notebook		
			where they can run the		
			VQL query invoking the		
			copy() VQL function.		
			Typically, most users		
			deploy Velociraptor		
			with limited access to a		
			trusted group (most		
			users will be		
			administrators within		
			the GUI). This		
			vulnerability is		
			associated with		
			program files		
			https://github.Com/Vel		

0-1

1-2

2-3

3-4 4-5 Page **286** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ocidex/velociraptor/bl ob/master/vql/filesyst em/copy.go https://github.Com/Vel ocidex/velociraptor/bl ob/master/vql/filesyst em/copy.go and program routines copy(). This issue affects Velociraptor versions before 0.6.7-5. Version 0.6.7-5, released January 16, 2023, fixes the issue. CVE ID : CVE-2023-		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Jan-2023	4.3	0242 Rapid7 Velociraptor did not properly sanitize the client ID parameter to the CreateCollection API, allowing a directory traversal in where the collection task could be written. It was possible to provide a client id of "/clients/server" to schedule the collection for the server (as a server artifact), but only require privileges to schedule collections on the client. Normally, to schedule an artifact on the server, the COLLECT_SERVER permission is required. This permission is normally only granted to "administrator" role. Due to this issue, it is sufficient to have the COLLECT_CLIENT	N/A	A-RAP-VELO- 020223/423

0-1

1-2

 2-3
 3-4
 4-5

 Page 287 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege, which is normally granted to the "investigator" role. To exploit this vulnerability, the attacker must already have a Velociraptor user account at least "investigator" level, and be able to authenticate to the GUI and issue an API call to the backend. Typically, most users deploy Velociraptor with limited access to a trusted group, and most users will already be administrators within the GUI. This issue affects Velociraptor versions before 0.6.7-5. Version 0.6.7-5, released January 16, 2023, fixes the issue. CVE ID : CVE-2023- 0290		
Vendor: Red	dhat				
Product: op	enshift				
Affected Ver	sion(s): 4.11				
Use of a Broken or Risky Cryptograp hic Algorithm	17-Jan-2023	5.3	The Birthday attack against 64-bit block ciphers flaw (CVE- 2016-2183) was reported for the health checks port (9979) on etcd grpc-proxy component. Even though the CVE-2016- 2183 has been fixed in the etcd components, to enable periodic health checks from kubelet, it	N/A	A-RED- OPEN- 020223/424

0-1

1-2

 2-3
 3-4
 4-5

 Page 288 of 463

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			was necessary to open up a new port (9979) on etcd grpc-proxy, hence this port might be considered as still vulnerable to the same type of vulnerability. The health checks on etcd grpc-proxy do not contain sensitive data (only metrics data), therefore the potential impact related to this vulnerability is minimal. The CVE- 2023-0296 has been assigned to this issue to track the permanent fix in the etcd component. CVE ID : CVE-2023- 0296					
Vondor: roc	kstargames		0296					
	and_theft_auto	V						
Affected Ver		_*						
N/A	22-Jan-2023	7.3	Grand Theft Auto V for PC allows attackers to achieve partial remote code execution or modify files on a PC, as exploited in the wild in January 2023. CVE ID : CVE-2023- 24059	https://suppo rt.rockstarga mes.com/com munity/2000 63373/13252 523900819, https://suppo rt.rockstarga mes.com/com munity/2000 63373/13249 062368147	A-ROC- GRAN- 020223/425			
Vendor: sandhillsdev								
	sy_digital_dow							
Affected Ver	sion(s): * Up to	(excluding	g) 3.1.0.4					
Improper Neutralizat	20-Jan-2023	9.8	The Easy Digital Downloads WordPress	N/A	A-SAN-EASY- 020223/426			
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 289 of 463	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Plugin, version < 3.1.0.4, is affected by an unauthenticated SQL injection vulnerability in the 's' parameter of its 'edd_download_search' action.		
			CVE ID : CVE-2023- 23489		
Vendor: Sho	opware				
Product: sh	opware				
Affected Ver	sion(s): * Up to	(excluding	g) 6.4.18.1		
Insufficient Session Expiration	17-Jan-2023	9.8	Shopware is an open source commerce platform based on Symfony Framework and Vue js. The Administration session expiration was set to one week, when an attacker has stolen the session cookie they could use it for a long period of time. In version 6.4.18.1 an automatic logout into the Administration session has been added. As a result the user will be logged out when they are inactive. Users are advised to upgrade. There are no known workarounds for this issue. CVE ID : CVE-2023- 22732	https://docs.s hopware.com /en/shopwar e-6- en/security- updates/secu rity-update- 01- 2023?categor y=security- updates, https://githu b.com/shopw are/platform/ commit/cd7a 89cbcd3a042 8c6d1ef27b3a a15467a722ff 6	A-SHO-SHOP- 020223/427
Improper Control of Generation of Code	17-Jan-2023	8.8	Shopware is an open source commerce platform based on Symfony Framework	https://docs.s hopware.com /en/shopwar e-6-	A-SHO-SHOP- 020223/428

0-1

1-2

2-3

3-4 4-5 Page **290** of **463** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			and Vue js. In a Twig environment **without the Sandbox extension**, it is possible to refer to PHP functions in twig filters like `map`, `filter`, `sort`. This allows a template to call any global PHP function and thus execute arbitrary code. The attacker must have access to a Twig environment in order to exploit this vulnerability. This problem has been fixed with 6.4.18.1 with an override of the specified filters until the integration of the Sandbox extension has been finished. Users are advised to upgrade. Users of major versions 6.1, 6.2, and 6.3 may also receive this fix via a plugin. CVE ID : CVE-2023- 22731	en/security- updates/secu rity-update- 01- 2023?categor y=security- updates, https://githu b.com/shopw are/platform/ commit/89d1 ea154689cb6 202e0d3a0ce eae0febb0c09 e1	
Improper Input Validation	17-Jan-2023	7.5	Shopware is an open source commerce platform based on Symfony Framework and Vue js. In affected versions It was possible to put the same line item multiple times in the cart using the AP. The Cart Validators checked the line item's individuality and the user was able to bypass	https://docs.s hopware.com /en/shopwar e-6- en/security- updates/secu rity-update- 01- 2023?categor y=security- updates, https://githu b.com/shopw	A-SHO-SHOP- 020223/429

0-1

1-2

2-33-44-5Page 291 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			quantity limits in sales. This problem has been fixed with version 6.4.18.1. Users on major versions 6.1, 6.2, and 6.3 may also obtain this fix via a plugin.	are/platform/ commit/4fce1 2096e54b203 3832d9104fa 2e68888c2b4 e9	
			CVE ID : CVE-2023- 22730		
Improper Input Validation	17-Jan-2023	7.5	Shopware is an open source commerce platform based on Symfony Framework and Vue js. The newsletter double opt- in validation was not checked properly, and it was possible to skip the complete double opt in process. As a result operators may have inconsistencies in their newsletter systems. This problem has been fixed with version 6.4.18.1. Users are advised to upgrade. Users unable to upgrade may find security measures are available via a plugin for major versions 6.1, 6.2, and 6.3. Users may also disable newsletter registration completely. CVE ID : CVE-2023- 22734	https://docs.s hopware.com /en/shopwar e-6- en/security- updates/secu rity-update- 01- 2023?categor y=security- updates, https://githu b.com/shopw are/platform/ commit/f5a9 5ee2bcf1e546 878450963ef 1d9886e59a6 20	A-SHO-SHOP- 020223/430
Insertion of Sensitive Informatio n into Log File	17-Jan-2023	6.5	Shopware is an open source commerce platform based on Symfony Framework and Vue js. In affected versions the log module	https://githu b.com/shopw are/platform/ commit/407a 83063d7141c 1a626441799	A-SHO-SHOP- 020223/431

0-1

1-2

2-3

3-4 4-5 Page **292** of **463** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would write out all kind of sent mails. An attacker with access to either the local system logs or a centralized logging store may have access to other users accounts. This issue has been addressed in version 6.4.18.1. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. Users unable to upgrade may remove from all users the log module ACL rights or disable logging. CVE ID : CVE-2023- 22733	c3ebef79498c 07, https://docs.s hopware.com /en/shopwar e-6- en/security- updates/secu rity-update- 01- 2023?categor y=security- updates	
Vendor: sig	nalwire			I	
Product: so	fia-sip				
Affected Ver	sion(s): * Up to	(excluding	g) 1.13.11		
Out-of- bounds Write	19-Jan-2023	9.8	Sofia-SIP is an open- source SIP User-Agent library, compliant with the IETF RFC3261 specification. In affected versions Sofia- SIP **lacks both message length and attributes length checks** when it handles STUN packets, leading to controllable heap-over-flow. For	https://githu b.com/freesw itch/sofia- sip/commit/d a53e4fbcb138 b080a75576d d49c1fff2ada 2764, https://githu b.com/freesw itch/sofia- sip/security/a dvisories/GH	A-SIG-SOFI- 020223/432

0-1

1-2

2-33-44-5Page 293 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			example, in stun_parse_attribute(), after we get the attribute's type and length value, the length will be used directly to copy from the heap, regardless of the message's left size. Since network users control the overflowed length, and the data is written to heap chunks later, attackers may achieve remote code execution by heap grooming or other exploitation methods. The bug was introduced 16 years ago in sofia-sip 1.12.4 (plus some patches through 12/21/2006) to in tree libs with git-svn-id: http://svn.freeswitch.o rg/svn/freeswitch/trun k@3774 d0543943- 73ff-0310-b7d9- 9358b9ac24b2. Users are advised to upgrade. There are no known workarounds for this vulnerability. CVE ID : CVE-2023- 22741	SA-8599- x7rq-fr54				
Vendor: stra	angerstudios							
Product: paid_memberships_pro								
Affected Ver	Affected Version(s): * Up to (excluding) 2.9.8							
Improper Neutralizat ion of Special	20-Jan-2023	9.8	The Paid Memberships Pro WordPress Plugin, version < 2.9.8, is affected by an	N/A	A-STR-PAID- 020223/433			

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4
 4-5
 5-6
 6-7
 7-8
 8-9
 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			unauthenticated SQL injection vulnerability in the 'code' parameter of the '/pmpro/v1/order' REST route. CVE ID : CVE-2023-		
			23488		
Vendor: sud					
Product: su					
Affected Ver	sion(s): 1.9.12			Γ	
Improper Privilege Manageme nt	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user- specified editor may contain a "" argument that defeats a protection mechanism, e.g., an EDITOR='vim /path/to/extra/file' value. CVE ID : CVE-2023- 22809	https://www. sudo.ws/secu rity/advisorie s/sudoedit_an y/, https://securi ty.netapp.com /advisory/nta p-20230127- 0015/	A-SUD-SUDO- 020223/434
Affected Ver	sion(s): From (i	ncluding)	1.8.0 Up to (excluding) 1.9	0.12	

0-1

1-2

 2-3
 3-4
 4-5

 Page 295 of 463

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Manageme nt	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user- specified editor may contain a "" argument that defeats a protection mechanism, e.g., an EDITOR='vim /path/to/extra/file' value. CVE ID : CVE-2023- 22809	https://www. sudo.ws/secu rity/advisorie s/sudoedit_an y/, https://securi ty.netapp.com /advisory/nta p-20230127- 0015/	A-SUD-SUDO- 020223/435
Vendor: Ter	nable				
Product: ne					
Affected Ver	sion(s): From (i	ncluding)	10.0.0 Up to (excluding) 1	0.4.2	
Improper Privilege Manageme nt	20-Jan-2023	8.8	A privilege escalation vulnerability was identified in Nessus versions 8.10.1 through 8.15.8 and 10.0.0 through 10.4.1. An authenticated attacker could potentially execute a specially crafted file to obtain root or NT AUTHORITY	https://www. tenable.com/s ecurity/tns- 2023-02, https://www. tenable.com/s ecurity/tns- 2023-01	A-TEN-NESS- 020223/436

0-1

1-2

 2-3
 3-4
 4-5

 Page
 296 of
 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/ SYSTEM privileges on the Nessus host.		
			CVE ID : CVE-2023- 0101		
Affected Vers	sion(s): From (i	ncluding)	8.10.1 Up to (excluding) 8	.15.8	
Improper Privilege Manageme nt	20-Jan-2023	8.8	A privilege escalation vulnerability was identified in Nessus versions 8.10.1 through 8.15.8 and 10.0.0 through 10.4.1. An authenticated attacker could potentially execute a specially crafted file to obtain root or NT AUTHORITY / SYSTEM privileges on the Nessus host. CVE ID : CVE-2023- 0101	https://www. tenable.com/s ecurity/tns- 2023-02, https://www. tenable.com/s ecurity/tns- 2023-01	A-TEN-NESS- 020223/437
	radsystem_pro	oject			
Product: the					
Affected Ver	sion(s): * Up to	(excluding	g) 2015-04-03		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2023	6.1	A vulnerability was found in saemorris TheRadSystem. It has been classified as problematic. Affected is an unknown function of the file users.php. The manipulation of the argument q leads to cross site scripting. It is possible to launch the attack remotely. VDB- 218454 is the identifier assigned to this vulnerability. CVE ID : CVE-2023- 0327	https://githu b.com/saemo rris/TheRadS ystem/commi t/bfba26bd34 af31648a11af 35a0bb66f19 48752a6	A-THE- THER- 020223/438

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Vendor: tpn	n2_software_st	ack_proj	ect	L	L				
Product: tp	Product: tpm2_software_stack								
Affected Ver	sion(s): * Up to	(including	g) 4.0.0						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Jan-2023	6.4	tpm2-tss is an open source software implementation of the Trusted Computing Group (TCG) Trusted Platform Module (TPM) 2 Software Stack (TSS2). In affected versions `Tss2_RC_SetHandler` and `Tss2_RC_Decode` both index into `layer_handler` with an 8 bit layer number, but the array only has `TPM2_ERROR_TSS2_R C_LAYER_COUNT` entries, so trying to add a handler for higher- numbered layers or decode a response code with such a layer number reads/writes past the end of the buffer. This Buffer overrun, could result in arbitrary code execution. An example attack would be a MiTM bus attack that returns 0xFFFFFFF for the RC. Given the common use case of TPM modules an attacker must have local access to the target machine with local system privileges which allows access to the TPM system. Usually TPM access	https://githu b.com/tpm2- software/tpm 2- tss/commit/3 06490c8d848 c367faa2d9df 81f5e69dab4 6ffb5	A-TPM- TPM2- 020223/439				

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requires administrative privilege.		
			CVE ID : CVE-2023- 22745		
Vendor: tre					
-	yhigh_secure_v	web_gate	way		
Affected Ver	sion(s): 12.0.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	6.1	A cross-site scripting vulnerability in Skyhigh SWG in main releases 11.x prior to 11.2.6, 10.x prior to 10.2.17, and controlled release 12.x prior to 12.0.1 allows a remote attacker to craft SWG- specific internal requests with URL paths to any third-party website, causing arbitrary content to be injected into the response when accessed through SWG.	https://kcm.t rellix.com/cor porate/index? page=content &id=SB10393	A-TRE-SKYH- 020223/440
			0214		
Affected Ver	sion(s): From (i	ncluding)	10.0.0 Up to (excluding) 1	0.2.17	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	6.1	A cross-site scripting vulnerability in Skyhigh SWG in main releases 11.x prior to 11.2.6, 10.x prior to 10.2.17, and controlled release 12.x prior to 12.0.1 allows a remote attacker to craft SWG- specific internal requests with URL paths to any third-party website, causing arbitrary content to be	https://kcm.t rellix.com/cor porate/index? page=content &id=SB10393	A-TRE-SKYH- 020223/441

0-1

1-2

2-3

3-4 4-5 Page **299** of **463** 5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the response when accessed through SWG.		
			CVE ID : CVE-2023- 0214		
Affected Ver	sion(s): From (i	ncluding)	11.0.0 Up to (excluding) 1	1.2.6	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	6.1	A cross-site scripting vulnerability in Skyhigh SWG in main releases 11.x prior to 11.2.6, 10.x prior to 10.2.17, and controlled release 12.x prior to 12.0.1 allows a remote attacker to craft SWG- specific internal requests with URL paths to any third-party website, causing arbitrary content to be injected into the response when accessed through SWG. CVE ID : CVE-2023- 0214	https://kcm.t rellix.com/cor porate/index? page=content &id=SB10393	A-TRE-SKYH- 020223/442
Vendor: Tru	istwave				
Product: mo	odsecurity				
Affected Ver	sion(s): * Up to	(excluding	g) 2.9.7		
N/A	20-Jan-2023	9.8	Incorrect handling of '\0' bytes in file uploads in ModSecurity before 2.9.7 may allow for Web Application Firewall bypasses and buffer overflows on the Web Application Firewall when executing rules that read the FILES_TMP_CONTENT collection.	https://githu b.com/Spider Labs/ModSec urity/pull/28 57/commits/ 4324f0ac59f8 225aa44bc50 34df60dbeccd 1d334, https://githu b.com/Spider Labs/ModSec	A-TRU- MODS- 020223/443

0-1

1-2

 2-3
 3-4
 4-5

 Page 300 of 463

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24021	urity/pull/28 57	
Vendor: twi	nkletoessoftw	are		•	
Product: bo	oked				
Affected Ver	sion(s): 2.5.5				
N/A	22-Jan-2023	4.3	Booked Scheduler 2.5.5 allows authenticated users to create and schedule events for any other user via a modified userId value to reservation_save.php. NOTE: 2.5.5 is a version from 2014; the latest version of Booked Scheduler is not affected. However, LabArchives Scheduler (Sep 6, 2022 Feature Release) is affected. CVE ID : CVE-2023- 24058	https://www. labarchives.co m/labarchive s-knowledge- base/2022- feature- releases-2/, https://www. bookedsched uler.com/the- future-of- booked/	A-TWI- BOOK- 020223/444
Vendor: uni	istra				
Product: im	patient				
Affected Ver	sion(s): * Up to	(excluding	g) 1.5.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	7.6	IMPatienT before 1.5.2 allows stored XSS via onmouseover in certain text fields within a PATCH /modify_onto request to the ontology builder. This may allow attackers to steal Protected Health Information. CVE ID : CVE-2023- 23637	https://githu b.com/lambd a- science/IMPat ienT/issues/1 01, https://githu b.com/lambd a- science/IMPat ienT/compare /v1.5.1v1.5. 2, https://githu b.com/lambd	A-UNI-IMPA- 020223/445

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				a- science/IMPat ienT/releases /tag/v1.5.2	
Vendor: VIN					
Product: vii					
Affected Ver	sion(s): * Up to	(excluding	g) 9.0.1225		
Heap- based Buffer Overflow	21-Jan-2023	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1225. CVE ID : CVE-2023- 0433	https://githu b.com/vim/vi m/commit/11 977f917506d 950b7e0cae5 58bd9189260 b253b, https://huntr. dev/bounties /ae933869- a1ec-402a- bbea- d51764c6618 e	A-VIM-VIM- 020223/446
Vendor: wa	rfareplugins				
Product: so	cial_warfare				
Affected Ver	sion(s): * Up to	(excluding	g) 4.4.0		
Cross-Site Request Forgery (CSRF)	19-Jan-2023	5.4	The Social Warfare plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.4.0. This is due to missing or incorrect nonce validation on several AJAX actions. This makes it possible for unauthenticated attackers to delete post meta information and reset network access tokens, via forged request granted they	N/A	A-WAR-SOCI- 020223/447

0-1

1-2

 2-3
 3-4
 4-5

 Page 302 of 463

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can trick a site administrator into performing an action such as clicking on a link. CVE ID : CVE-2023-		
			0403		
Affected Ver	sion(s): * Up to	(including	g) 4.3.0		
Missing Authorizati on	19-Jan-2023	5.4	The Social Warfare plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on several AJAX actions in versions up to, and including, 4.3.0. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete post meta information and reset network access tokens. CVE ID : CVE-2023- 0402	https://plugin s.trac.wordpr ess.org/chang eset?sfp_email =&sfph_mail= &reponame= &old=284409 2%40social- warfare&new =2844092%4 0social- warfare&sfp_ email=&sfph_ mail=	A-WAR-SOCI- 020223/448
Vendor: Wi	reshark				
Product: wi					
Affected Ver	sion(s): From (i	ncluding)	3.6.0 Up to (including) 3.6		
Excessive Iteration	26-Jan-2023	6.5	Excessive loops in multiple dissectors in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023-	https://www. wireshark.org /security/wn pa-sec-2023- 06.html, https://gitlab. com/wireshar k/wireshark/ - /issues/1873	A-WIR- WIRE- 020223/449
			0411	7, https://gitlab.	

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/wireshar k/wireshark/ - /issues/1871 1, https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0411.json	
Improper Resource Shutdown or Release	26-Jan-2023	6.5	TIPC dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0412	https://gitlab. com/wireshar k/wireshark/ - /issues/1877 0, https://www. wireshark.org /security/wn pa-sec-2023- 07.html, https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0412.json	A-WIR- WIRE- 020223/450
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Dissection engine bug in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0413	https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0413.json, https://www. wireshark.org /security/wn pa-sec-2023- 03.html, https://gitlab.	A-WIR- WIRE- 020223/451

0-1

1-2

2-3

3-4 4-5 Page **304** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/wireshar k/wireshark/ - /issues/1876 6	
Improper Resource Shutdown or Release	26-Jan-2023	6.5	iSCSI dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0415	https://gitlab. com/wireshar k/wireshark/ - /issues/1879 6, https://www. wireshark.org /security/wn pa-sec-2023- 05.html, https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0415.json	A-WIR- WIRE- 020223/452
Improper Resource Shutdown or Release	26-Jan-2023	6.5	GNW dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0416	https://gitlab. com/wireshar k/wireshark/ - /issues/1877 9, https://www. wireshark.org /security/wn pa-sec-2023- 04.html, https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0416.json	A-WIR- WIRE- 020223/453

0-1

1-2

2-33-44-5Page 305 of 463

5-6

6-7

7-8 8-9

0-1

1-2

 2-3
 3-4
 4-5

 Page 306 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	26-Jan-2023	6.5	TIPC dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0412	https://gitlab. com/wireshar k/wireshark/ - /issues/1877 0, https://www. wireshark.org /security/wn pa-sec-2023- 07.html, https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0412.json	A-WIR- WIRE- 020223/456
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Dissection engine bug in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0413	https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0413.json, https://www. wireshark.org /security/wn pa-sec-2023- 03.html, https://gitlab. com/wireshar k/wireshark/ - /issues/1876 6	A-WIR- WIRE- 020223/457
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Crash in the EAP dissector in Wireshark 4.0.0 to 4.0.2 allows denial of service via packet injection or crafted capture file	https://www. wireshark.org /security/wn pa-sec-2023- 01.html, https://gitlab. com/gitlab-	A-WIR- WIRE- 020223/458

0-1

1-2

2-3

3-4 4-5 Page **307** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0414	org/cves/- /blob/master /2023/CVE- 2023- 0414.json, https://gitlab. com/wireshar k/wireshark/ - /issues/1862 2	
Improper Resource Shutdown or Release	26-Jan-2023	6.5	iSCSI dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0415	https://gitlab. com/wireshar k/wireshark/ - /issues/1879 6, https://www. wireshark.org /security/wn pa-sec-2023- 05.html, https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0415.json	A-WIR- WIRE- 020223/459
Improper Resource Shutdown or Release	26-Jan-2023	6.5	GNW dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0416	https://gitlab. com/wireshar k/wireshark/ - /issues/1877 9, https://www. wireshark.org /security/wn pa-sec-2023- 04.html, https://gitlab. com/gitlab- org/cves/-	A-WIR- WIRE- 020223/460

0-1

1-2

2-3

3-4 4-5 Page **308** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
				/blob/master /2023/CVE- 2023- 0416.json		
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Memory leak in the NFS dissector in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file CVE ID : CVE-2023- 0417	https://www. wireshark.org /security/wn pa-sec-2023- 02.html, https://gitlab. com/wireshark/ - /issues/1862 8, https://gitlab. com/gitlab- org/cves/- /blob/master /2023/CVE- 2023- 0417.json	A-WIR- WIRE- 020223/461	
	_topbar_projec	t				
Product: wp	-					
Affected Vers	sion(s): * Up to	(including	g) 5.36			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	23-Jan-2023	8.8	Auth. SQL Injection (SQLi) vulnerability in WP-TopBar <= 5.36 versions. CVE ID : CVE-2023- 23824	N/A	A-WP WP_T- 020223/462	
Vendor: youtube_shortcode_project						
Product: youtube_shortcode						
Affected Vers	sion(s): * Up to	(including	g) 1.8.5			

0-1

1-2

2-3

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2023	5.4	Auth. Stored Cross-Site Scripting (XSS) vulnerability in Youtube shortcode <= 1.8.5 versions. CVE ID : CVE-2023- 23687	N/A	A-YOU- YOUT- 020223/463	
Vendor: zdi	r_project					
Product: zd	ir					
Affected Ver	sion(s): 3.2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2023	8.8	An arbitrary file upload vulnerability in the /api/upload component of zdir v3.2.0 allows attackers to execute arbitrary code via a crafted .ssh file. CVE ID : CVE-2023- 23314	https://githu b.com/helloxz /zdir/issues/ 90	A-ZDI-ZDIR- 020223/464	
Vendor: Zol	nocorp					
Product: ma	anageengine_e	xchange_	reporter_plus			
Affected Ver	sion(s): * Up to	(excludin	g) 5.7			
Improper Restriction of XML External Entity Reference	17-Jan-2023	7.5	Zoho ManageEngine Exchange Reporter Plus before 5708 allows attackers to conduct XXE attacks. CVE ID : CVE-2023- 22624	https://www. manageengin e.com/produc ts/exchange- reports/advis ory/CVE- 2023- 22624.html	A-ZOH- MANA- 020223/465	
Affected Version(s): 5.7						
Improper Restriction of XML External Entity Reference	17-Jan-2023	7.5	Zoho ManageEngine Exchange Reporter Plus before 5708 allows attackers to conduct XXE attacks.	https://www. manageengin e.com/produc ts/exchange- reports/advis ory/CVE-	A-ZOH- MANA- 020223/466	

0-1

1-2

5-6

6-7

Authentica tion20-Jan-20239.1authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023- 22964ttyserVice- desk- msp/cve- 2023- 22964.htmlMANA- 020223/467Affected Version(s): 13.0Zoho ManageEngine ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023- 22964https://www. managegnine e.com/produc ts/service- desk- msp/cve- 2023- 22964.htmlA-ZOH- MANA- 020223/467Improper Authentica tion20-Jan-20239.1Zoho ManageEngine ServiceDesk Plus MSP before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023- 22964https://www. managegnine e.com/produc ts/service- desk- msp/cve- 2023- 22964.htmlA-ZOH- MANA- 020223/468Improper Vendor: ate-mahorobaVer ID : CVE-2023- 229642094.htmlA-ZOH- MANA- 020223/468Improper Neutralizat ion of Special ElementsI7-Jan-20239.8MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, mahoroba.jp/ netdevancer/ mahoroba.jp/ netdevancer/ mahoroba.jp/ netdevancer/ manual/H-ATE- MAHO- 020223/469	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.6 Zoho ManageEngine ServiceDesk Plus MSP before 10611, and 13x before 1004, is vulnerable to authentication bypass when LDAP authentication is enabled. https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023.22964 A-ZOH- MANA- 020223/467 Affected Version(s): 13.0 Zoho ManageEngine ServiceDesk Plus MSP before 1004, is uuthentication is enabled. https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023.22964 A-ZOH- MANA- 020223/467 Affected Version(s): 13.0 Zoho ManageEngine ServiceDesk Plus MSP before 1004, is vulnerable to authentication is enabled. https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023- 22964 A-ZOH- MANA- 020223/467 Improper Authentica tion 20-Jan-2023 9.1 Zoho ManageEngine ServiceDesk Plus MSP before 1004, is when LDAP authentication bypass when LDAP authentication is enabled. https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023- 22964 Vendor: ate-mahoroba Hardware Hardware Vendor: ate-mahoroba NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, NetDevancer VSG Lite/Uni prior to Ver.1.11.00, netdevancer/ manual/ H-ATE- MAHO- 020223/469						
Improper Authentica tion20-Jan-20239.1Zoho ManageEngine ServiceDesk Plus MSP before 13004, is uulnerable to authentication bypass when LDAP authentication is enabled.https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023- 22964.htmlA-ZOH- MANA- 020223/467Affected Version(s): 13.0Zoho ManageEngine ServiceDesk Plus MSP before 10611, and 13x before 10610, and 14x before 10610, and MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, and MAHO- netdevancer/ manual/A-ZOH- MAHO- MAHO- MAHO-PBX NetDevancer MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancerhttps://www. ate- mahoroba.jp/ MAHO- 020223/469	Product: ma	anageengine_s	ervicedes	k_plus_msp		
Improper Authentica tion20-Jan-20239,1ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled.https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023- 22964.htmlA:ZOH- MANA- 020223/467Affected Version(s): 13.0CVE ID : CVE-2023- 22964https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023- 22964.htmlA:ZOH- MANA- 020223/467Improper Authentica tion20-Jan-20239,1Zoho ManageEngin ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023- 22964.htmlA:ZOH- MANA- 020223/468Improper Authentica tion9,1Zoho ManageEngin ServiceDesk Plus MSP before 13004, is vulnerable to authentication bypass when LDAP authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023- 22964.htmlA:ZOH- MANA- 020223/468Improper Netorer Netorer Netorer Netorer Netorer Secial ElementsMAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.111.00, endboroba.jp/ netdevancer/ manual/H:ATE- MAHO- 020223/469Improper Netorevancer9,8MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.111.00, and MAHO- PBX NetDevancerhttps://www. anual/	Affected Ver	sion(s): 10.6				
Improper Authentica tion20-Jan-20239.1Zoho ManageEngine ServiceDesk Plus MSP before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023- 22964https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023- 22964.htmlA-ZOH- MANA- 020223/468Vendor: ate-mahorobaMAHO-PBX NetDevancerMAHO-PBX NetDevancerAtfected Version(s): -Improper Neutralizat ion of Special Elements used in an OS Command (OSMAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancerhttps://www. ate- mahoroba.jp/ mathoroba.jp/ mathoroba.jp/ manual/H-ATE- MAHO- 020223/469	Improper Authentica tion	20-Jan-2023	9.1	ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023-	manageengin e.com/produc ts/service- desk- msp/cve- 2023-	MANA-
Improper Authentica tion20-Jan-20239.1ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023- 22964https://www. manageengin e.com/produc ts/service- desk- msp/cve- 2023- 22964.htmlA-ZOH- MANA- 020223/468Vendor: ate-mahorobaMAHO-PBX NetDevancerMAHO-PBX NetDevancerMAHO-PBX NetDevancerH-ATE- mahoroba.jp/ netdevancer/ MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancerhttps://www. ate- mahoroba.jp/ netdevancer/ MAHO-020223/469	Affected Ver	sion(s): 13.0				
Vendor: ate-mahorobaProduct: maho-pbx_netdevancerAffected Version(s): -Improper Neutralizat ion of Special Elements used in an OS Command ('OSMAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancerhttps://www. ate- mahoroba.jp/ netdevancer/ manual/	Improper Authentica tion	20-Jan-2023	9.1	ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. CVE ID : CVE-2023-	manageengin e.com/produc ts/service- desk- msp/cve- 2023-	MANA-
Product: maho-pbx_netdevancer Affected Version(s): - Improper Neutralization of Special Elements 17-Jan-2023 9.8 MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to OS Command ('OS				Hardware		
Affected Version(s): - Improper Neutralizat ion of Special Elements used in an OS Command ('OS Special Command	Vendor: ate	-mahoroba				
Improper Neutralizat ion of Special Elements used in an OS Command ('OSMAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancerhttps://www. ate- mahoroba.jp/ netdevancer/ 020223/469	Product: ma	aho-pbx_netde	vancer			
Neutralizat ion of Special Elements used in an OS Command ('OSNetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancerhttps://www. ate- mahoroba.jp/ MAHO- 020223/469	Affected Ver	sion(s): -				
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Improper Neutralizat ion of Special Elements used in an OS Command ('OS	17-Jan-2023	9.8	NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-	ate- mahoroba.jp/ netdevancer/	MAHO-
	CVSS Scoring	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page **311** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command.		
			CVE ID : CVE-2023- 22279		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO- PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. CVE ID : CVE-2023- 22286	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/470
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/471

0-1

1-2

2-3

3-4 4-5 Page **312** of **463** 7-8

5-6

8-9 9-10

		Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege to execute an arbitrary		
		OS command. CVE ID : CVE-2023- 22280		
17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVE ID : CVE-2023- 22296	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/472
ho-pbx_netde	vancer_m	obilegate		
ion(s): -				
17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/473
	ho-pbx_netdev ion(s): -	ho-pbx_netdevancer_m ion(s): - 17-Jan-2023 9.8	17-Jan-20236.1scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVE ID : CVE-2023- 22296tor(s): -MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, and MAHO-PBX NetDevancer NetDevancer17-Jan-20239.8MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, and MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, and MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, mAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, and MAHO-PBX NetDevancer Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer NetDevancer MobileGate Home/Office prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to	17-Jan-20236.1scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVF ID : CVE-2023- 22296https://www. ate- mahoroba.jp/ netdevancer/ manual/tor.pbx_netdevancer_mobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVF ID : CVE-2023- 22296https://www. ate- manual/tor.gli>tor.joMAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MAHO-PBX NetDevancer Mahoroba.jp/ netdevancer/ manual/

Page **313** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command. CVE ID : CVE-2023-		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	22279 Cross-site request forgery (CSRF) vulnerability in MAHO- PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. CVE ID : CVE-2023- 22286	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/474
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/475

0-1

1-2

2-3

3-4 4-5 Page **314** of **463** 6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with an administrative privilege to execute an arbitrary OS command. CVE ID : CVE-2023- 22280		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVE ID : CVE-2023- 22296	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/476
Product: ma	aho-pbx_netde	vancer_v	sg		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/477

0-1

1-2

2-33-44-5Page 315 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute an arbitrary OS command. CVE ID : CVE-2023-		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	CVE ID : CVE-2023- 22279 Cross-site request forgery (CSRF) vulnerability in MAHO- PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in.	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/478
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	CVE ID : CVE-2023- 22286 MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege	https://www. ate- mahoroba.jp/ netdevancer/ manual/	H-ATE- MAHO- 020223/479

0-1

1-2

2-3

3-4 4-5 Page **316** of **463** 6-7

5-6

7-8

8-9

Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') 17-Jan-2023 6.1 17-Jan-2023 6.1 17-Jan-2023 6.1 6.1 4.1 4.1 4.4 4.4 4.4 4.4 4.4 4	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation (Cross-site Scripting')17-Jan-20236.1scripting vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer Ver.1.11.00, and MAHO- PBX NetDevancer Ver.1.11.00 and MAHO- PBX NetDevancer Ver.1.11.00 and MAHO- PBX NetDevancer Ver.1.11.00 and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated atacker to inject an arbitrary script. CVE ID : CVE-2023- 22296H-ATE- MAHO- 020223/480Vendor: CiscoVendor: CiscoVendor: CiscoImproper Neutralizat ion of Special Elements in Output Used by a Downstrea mA vulnerability in the URL filtering mechanism of Cisco Async0S Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL remote attacker to bypass-WbMQaNJhH-CIS-EMAI- D0223/481				OS command. CVE ID : CVE-2023-		
Product: email_security_appliance_c160Affected Version(s): -Improper Neutralizat ion of Special 	Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVE ID : CVE-2023-	ate- mahoroba.jp/ netdevancer/	MAHO-
Affected Version(s): -Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m t t ('Injection')A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJhH-CIS-EMAI- 020223/481	Vendor: Cis	со				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m ('Injection')A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, reputation filters on an affected device. This vulnerability is due to improper processing ofhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJhH-CIS-EMAI- 020223/481	Product: en	nail_security_a	ppliance_	c160		
Neutralizat ion of Special Elements in Output Used by a Downstrea m ('Injection')	Affected Ver	sion(s): -				
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	('Injection'	20-Jan-2023	5.3	URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass-	
	CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page **317** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. CVE ID : CVE-2023- 20057		
Product: en	nail_security_a	ppliance			
Affected Ver					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/482

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious URLs to pass through the device.		
			CVE ID : CVE-2023- 20057		
Product: em	nail_security_a	ppliance_	c190		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. CVE ID : CVE-2023- 20057	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/483
Affected Ver		ppnance_			
Improper Neutralizat ion of Special	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for	https://sec.cl oudapps.cisco .com/security /center/conte	H-CIS-EMAI- 020223/484

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstrea m Componen t ('Injection')			Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. CVE ID : CVE-2023- 20057	nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	
Product: em	nail_security_a	ppliance_	c370d		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/485

0-1

1-2

2-3

3-4 4-5 Page **320** of **463** 8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.		
			CVE ID : CVE-2023- 20057		
Product: en	nail_security_a	ppliance_			
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/486

0-1

1-2

3-4 4-5 Page **321** of **463**

2-3

6-7 7-8

5-6

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20057		
Product: en	nail_security_a	ppliance_	<u>.</u> c390	L	I
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. CVE ID : CVE-2023- 20057	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/487
	nail_security_a	ppliance_	<u>.</u> c670		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa-	H-CIS-EMAI- 020223/488
CVSS Scoring S	Scale 0-1	1-2 2	- 3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstrea m Componen t ('Injection')			unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. CVE ID : CVE-2023- 20057	url-bypass- WbMQqNJh	
Product: en	nail_security_a	ppliance_	c680		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/489

0-1

1-2

2-3

3-4 4-5 Page **323** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Des	scription & (CVE ID		Patch		NCII	PC ID
			attack URL r that a an aff which malici	it could all ter to bypa eputation re configu ected devi could allo ious URLs gh the dev	nss the filters red for ce, ow to pass					
			CVE II 2005	D : CVE-2(7)23-					
Product: em	nail_security_a	ppliance_	_c690							
Affected Vers	sion(s): -					-				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	URL fi mecha Async Cisco Applia allow unaut remot bypas reputa affecto vulnes affecto vulnes a URLs. exploi vulnes a URL way. A exploi attack URL r that a an affe which malici throus CVE II 2005	henticated te attacker as the URL ation filter ed device. rability is o per proce An attacko it this rability by in a partic st could all ter to bypa eputation re configu ected devic could all tous URLs gh the dev D : CVE-20	isco re for urity could d, to rs on an This due to ssing of er could crafting cular ul ow the iss the filters red for ce, ow to pass ice.	ouda .com /cen nt/C ityAd sco-s url-b	s://sec apps.cis /secur ter/con iscoSec dvisory sa-esa- oypass- 1QqNJh	sco ity nte cur y/ci	H-CIS- 02022	
Product: em	nail_security_a	ppliance_	<u>.</u> c690x							
CVSS Scoring S	Scale 0-1	1-2 2	2-3	3-4 4-5	5-6	6-	7 7	7-8	8-9	9-10

Page 324 of 463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -		L	L	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. CVE ID : CVE-2023- 20057	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/491
Product: en	nail_security_a	ppliance_	x1070		
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	H-CIS-EMAI- 020223/492

0-1

1-2

2-3

3-4 4-5 Page **325** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.		
			CVE ID : CVE-2023- 20057		
Product: ip_	phones_8832				
Affected Ver	sion(s): -				
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/493

0-1

1-2

2-3

3-4 4-5 Page **326** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain parts of the web interface that would normally require authentication.		
			CVE ID : CVE-2023- 20018		
Product: ip_	phone_7800				
Affected Vers	sion(s): -				
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/494
Product: ip_	phone_7811				
Affected Vers	sion(s): -				
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface	https://sec.cl oudapps.cisco .com/security	H-CIS-IP_P- 020223/495
CVSS Scoring S	cale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page **327** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	/center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	
Product: ip_	phone_7821				
Affected Ver	sion(s): -				
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/496

0-1

1-2

2-3

3-4 4-5 Page **328** of **463** 5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018		
Product: in	_phone_7832		20010		
Affected Ver					
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/497

0-1

1-2

2-33-44-5Page 329 of 463

6-7 7-8

5-6

Authorizati on20-Jan-20236.5Supplied input Ait attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.nt/CliscoSecur ityAdvisory/ci phone-auth- bypass- pSqxZRPRH-CIS-IP_P- 020223/498Product: ip_phone_7861CVE ID : CVE-2023- 20018Soc-sa-ip- phone-auth- bypass- pSqxZRPRH-CIS-IP_P- ityAdvisory/ci phone-auth- bypass- pSqxZRPRIncorrect Authorizati on20-Jan-20236.5A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass- phone-auth- bypass- phone-auth- bypass- poqxZRPRH-CIS-IP_P- 020223/498	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorizati on20-Jan-2023A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is du validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the webi hattacker to access certain parts of the webi interface that would normally require authentication. CVE ID : CVE-2023- 20018https://sec.cl oudapps.cisco .com/security /center/conte mt/CiscoSecur phone-auth- bypass- pSqxZRPRH-CIS-IP_P- 020223/498Product: ip_bone_7861CVE ID : CVE-2023- 20018H-CIS-IP_P- (oudapps.cisco) .com/security /center/conte management interface of Cisco IP Phone 7800https://sec.cl oudapps.cisco .com/security /centre/conte nt/CiscoSecur .com/security /centre/conte nt/CiscoSecurity .com/security /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity /centre/conte nt/CiscoSecurity phone-auth- bypass- 	Product: ip_	phone_7841		L	L	I
Incorrect Authorization20-Jan-20236.5web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input An attacker could exploit this vulnerability by sending a crafted phone-auth- bypass.Ittps://se	Affected Ver	sion(s): -				
Affected Version(s): - Incorrect Authorizati on 20-Jan-2023 6.5 6.5 A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. Burget Phone Ph	Incorrect Authorizati on	20-Jan-2023	6.5	web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass-	_
Incorrect Authorizati on20-Jan-20236.5A vulnerability in the web-based of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device.https://sec.cl oudapps.cisco .com/security (center/conte nt/CiscoSecur ityAdvisory/ci bypass- phone-auth- bypass- pSqxZRPRH-CIS-IP_P- 020223/499	Product: ip_	phone_7861				
Incorrect Authorizati on20-Jan-20236.56.56.56.5and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device.H-CIS-IP_P- 020223/499	Affected Ver	sion(s): -				
	Incorrect Authorizati on	20-Jan-2023	6.5	web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass-	_
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				-3 3-4 4-5 5-6	6-7 7-8	

Page **330** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.		
			CVE ID : CVE-2023- 20018		
Product: ip_	phone_8800				
Affected Ver	sion(s): -			r	
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/500

0-1

1-2

2-3

3-4 4-5 Page **331** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			interface that would normally require authentication.						
			CVE ID : CVE-2023- 20018						
Product: ip_	phone_8811								
Affected Ver	sion(s): -			-					
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/501				
-	Product: ip_phone_8821 Affected Version(s): -								
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800	https://sec.cl oudapps.cisco .com/security /center/conte	H-CIS-IP_P- 020223/502				

0-1

1-2

2-33-44-5Page 332 of 463

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	
Product: ip	_phone_8821-e	X			
Affected Ver	<u> </u>				
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/503

0-1

1-2

2-3

3-4 4-5 Page **333** of **463** 6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-		
			20018		
	phone_8831				
Affected Vers	sion(s): -				
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/504
Product: ip_	phone_8832				
			-3 3-4 4-5 5-6	6-7 7-8	

Page **334** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): -								
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/505				
	phone_8841								
Affected Ver	sion(s): -								
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/506				

0-1

1-2

2-33-44-5Page 335 of 463

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.		
			CVE ID : CVE-2023- 20018		
-	phone_8845				
Affected Ver	sion(s): -		A 1 1:11: : .1		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/507

0-1

1-2

2-3

3-4 4-5 Page **336** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normally require authentication.		
			CVE ID : CVE-2023- 20018		
Product: ip_	phone_8851				
Affected Ver	sion(s): -				
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/508
-	phone_8861				
Affected Ver	sion(s): -		A uulnorability in the	https://soc.cl	
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	H-CIS-IP_P- 020223/509

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	
-	phone_8865				
Affected Ver			A vulnerability in the		
Incorrect Authorizati on	20-Jan-2023	6.5	web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-IP_P- 020223/510

0-1

1-2

2-3

3-4 4-5 Page **338** of **463** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-		
_			20018		
Product: rv					
Affected Ver			A vulnerability in the		
Improper Input Validation	20-Jan-2023	9.8	web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	H-CIS-RV01- 020223/511
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business	https://sec.cl oudapps.cisco .com/security /center/conte	H-CIS-RV01- 020223/512

0-1

1-2

 2-3
 3-4
 4-5

 Page 339 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. CVE ID : CVE-2023- 20026	nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	
Product: rv	042				L
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi-	H-CIS-RV04- 020223/513
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
		12 2	-5 5-4 4-5 5-0	3	

Page 340 of 463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025	vuln- ej76Pke5	
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	H-CIS-RV04- 020223/514

0-1

1-2

 2-3
 3-4
 4-5

 Page 341 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.		
			CVE ID : CVE-2023- 20026		
Product: rv	042g				
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	H-CIS-RV04- 020223/515
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci	H-CIS-RV04- 020223/516

0-1

1-2

2-33-44-5Page 342 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. CVE ID : CVE-2023- 20026	sco-sa- sbr042-multi- vuln- ej76Pke5	
Product: rv	082				
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	H-CIS-RV08- 020223/517
CV/SS Scaring (1_22		6.7 70	8_0 0.10
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 343 of 463	6-7 7-8	8-9 <mark>9-10</mark>

Page **343** of **463**

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025		
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	H-CIS-RV08- 020223/518

0-1

1-2

 2-3
 3-4
 4-5

 Page 344 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have valid Administrator credentials on the affected device.		
			CVE ID : CVE-2023- 20026		
Product: rv	160w_wireless	-ac_vpn_i	router	<u> </u>	
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-rv- cmd-exe- n47kJQLE	H-CIS-RV16- 020223/519

0-1

1-2

2-3

3-4 4-5 Page **345** of **463** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level credentials on the affected device.		
			CVE ID : CVE-2023- 20045		
Product: rv	160_vpn_route	r		·	
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator- level credentials on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-rv- cmd-exe- n47kJQLE	H-CIS-RV16- 020223/520

0-1

1-2

2-3

3-4 4-5 Page **346** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 20045					
Product: rv260p_vpn_router_with_poe								
Affected Version(s): -								
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator- level credentials on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-rv- cmd-exe- n47kJQLE	H-CIS-RV26- 020223/521			

0-1

1-2

2-3

3-4 4-5 Page **347** of **463** 5-6

Weakness	Publish Date	CVSSv3	Descript	ion & CVE	ID	Pat	ch	NCI	IPC ID
Affected Ver	sion(s): -								
Improper Input Validation	20-Jan-2023	7.2	A vulneral web-based manageme of Cisco Sr RV160 and Series VPN could allow authentica attacker to arbitrary of the underl operating affected de vulnerabil insufficien of user inp attacker co this vulner sending a request to based mar interface of device. A s exploit cou attacker to arbitrary of using root privileges affected de exploit thi vulnerabil attacker m valid Adm level crede affected de	d ent interf nall Busin d RV260 J Routers w an ited, rem o execute command ying system o evice. Thi ity is due t validation t validatio	face ness ote ls on f an is to ion oit y t tted l the ls	https:// oudapps .com/se /center, nt/Cisco ityAdvis sco-sa-r cmd-exe n47kJQI	s.cisco curity /conte oSecur sory/ci v- e-		-RV26- 23/522
Product: rv340									
Affected Ver	sion(s): -								
Improper Neutralizat	20-Jan-2023	7.2	A vulneral web-based	-	he	https:// oudapps			-RV34- 23/523
CVSS Scoring S	Scale 0-1	1-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

ion of Special Elements used in an (VS Command ('OS Command Injection')	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
management process to restart, resulting in a DoS condition. CVE ID : CVE-2023-	Special Elements used in an OS Command ('OS Command			of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. CVE ID : CVE-2023-	/center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos-	
20007						
Product: rv340w						
Affected Version(s): -	Affected Ver	sion(s): -				
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						8-9 9-10

Page 349 of 463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. CVE ID : CVE-2023- 20007	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos- 7HjP74jD	H-CIS-RV34- 020223/524

0-1

1-2

 2-3
 3-4
 4-5

 Page 350 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rv	345	I	L	L	I
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos- 7HjP74jD	H-CIS-RV34- 020223/525

0-1

1-2

2-3

3-4 4-5 Page **351** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 20007					
Product: rv	Product: rv345p							
Affected Ver	sion(s): -							
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos- 7HjP74jD	H-CIS-RV34- 020223/526			

0-1

1-2

2-3

3-4 4-5 Page **352** of **463** 6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			restart, resulting in a DoS condition.				
			CVE ID : CVE-2023- 20007				
Product: un	ified_ip_phone	_8851nr					
Affected Ver	Affected Version(s): -						
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-UNIF- 020223/527		
	ified_ip_phone	_8865nr					
Affected Vers Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	H-CIS-UNIF- 020223/528		

CVSS Scoring Scale	0-1	1-2	2-5	5-4	4-5	5-0	0-7	7-0
CVSS Scoring Scolo	0-1	1 2	22	2 /		56	67	70

8-9

Allocation of Resources Without 20-Jan-2023 6.5 A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Room Phone AD Room Phone A	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): - Affected Version(s): - A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service Limits or Allocation of Resources Without Limits or 20-Jan-2023 6.5				unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-	sco-sa-ip- phone-auth- bypass-	
Allocation of Resources Without Limits or20-Jan-20236.5A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on anhttps://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ciH-CIS-WEBE- 020223/529			one			
	of Resources Without	20-Jan-2023	6.5	Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service	oudapps.cisco .com/security /center/conte nt/CiscoSecur	

0-1

1-2

2-3

3-4 4-5 Page **354** of **463** 6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047		
Product: we					
Affected Ver	sion(s): -		A uniporchility in the		
Allocation of Resources Without Limits or Throttling	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-lldp- memlk- McOecPT	H-CIS-WEBE- 020223/530

0-1

1-2

2-3

3-4 4-5 Page **355** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047		
	reless_ip_phon	e_8821			
Affected Ver	sion(s): -		A mile or chility in the		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	H-CIS-WIRE- 020223/531

0-1

1-2

2-3

3-4 4-5 Page **356** of **463** 5-6

6-7

Incorrect Authorizati on20-Jan-20236.5A vulnerability in the veshing a crafted request to the web- based management interface that would normally require authentication. CVE ID : CVE-2023- 20018Https://sec.cl outdates of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface to the web- based management on an affected device. This vulnerability bis due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability bis due to insufficient validation of user- supplied input. An attacker could allow the attacker to access ccertain parts of the web- based management interface. A successful exploit could allow the attacker to access ccertain parts of the web- interface that would normally require authentication. CVF ID : CVE-2023- 20018H-CIS-WIRE- OU2023/532 sending a crafted request to the web- based management interface that would normally require authentication. CVF ID : CVE-2023- 20018H-CIS-WIRE- OU2023/532 sending a crafted request to the web- based management interface that would normally require authentication. CVF ID : CVE-2023- 20018H-CIS-WIRE- OU2023/532	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorizati on20-Jan-20236.5Associate Association could allow the attacker to access could allow the attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface that would normally require authentication. CVE ID : CVE-2023-https://sec.cl oudaps.cisco .com/security /center/conte ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPRH-CIS-WIRE- 020223/532				interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require		
Affected Version(s): -Affected Version(s): - <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
Incorrect Authorizati on20-Jan-2023A sulherability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An 	Product: wi	reless_ip_phon	e_8821-e	X		
Incorrect Authorizati on20-Jan-2023e.5web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.H-CIS-WIRE- 002223/532Incorrect AuthorizatiCVE ID : CVE-2023-H-CIS-WIRE- 00223/532	Affected Vers	sion(s): -				
Vendor: Dell	Authorizati on		6.5	web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass-	

0-1

1-2

2-3

3-4 4-5 Page **357** of **463** 6-7 7-8

5-6

nt Interpretat ion of HTTP Requests ('HTTP Requests Smuggling') 20-Jan-2023 20-Jan-2023 B.8 B.8 B.8 B.8 B.8 B.8 B.8 B.8	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inconsiste nt Interpretat ion of HTTP Requests Smuggling'20-Jan-20238.8Dell EMC PV ME5, versions ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and Dos.https://www. dell.com/sup ort/kbdoc/en is/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerabilityH-DEL- POWE- 020223/533Product: powervault_me5024Dell EMC PV ME5, versions ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attack- vulnerability to force a victim's browser to desynchronize its connection with the website.typically leading to XSS and Dos.H-DEL- POWE- 020223/533Product: powervault_me5024Dell EMC PV ME5, versions ME5.1.0.10, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the 	Product: po	wervault_me5	012		L	L
Inconsiste nt Interpretati ion of HTTP Requests (HTTP Request Smuggling')20-Jan-20238.8versions ME5.1.0.0. and ME5.1.0.1.0, contains a Client-side desync Vulherability. An unauthenticated attacker could potentially exploit this vulherability to force avictim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023- 23691https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerabilityhttps://www. dell.com/supp ort/kbdoc/en - us/00020753 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerabilityH-DEL- POWE- 020223/533Product: powervault_me5-24Dell EMC PV ME5, versions ME5.1.0.0, and ME5.1.0.10, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability of force avictim's browser to desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability of force avictim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023- 23691https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerability to force avictim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023- 23691https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a	Affected Ver	sion(s): -				
Affected Version(s): -Inconsiste nt Interpretati ion of HTTP Requests ('HTTP Requests ('HTTP Request ('HTTP Request ('HTTP Request Smuggling')20-Jan-20238.8Dell EMC PV ME5, versions ME5.1.0.0, and ME5.1.0.1,0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and Dos.https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerabilityProduct: powervault_me5084	Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023-	dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack-	POWE-
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')20-Jan-20238.8Dell EMC PV ME5, versions ME5.1.0.0, and ME5.1.0.1, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS.https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerabilityH-DEL- POWE- 020223/534Product: rowervault_me5084EVE ID : CVE-2023- 23691Ver ID : CVE-2023- 23691Ver ID : CVE-2023- 23691	Product: po	wervault_me5	024			
Inconsiste nt Interpretati ion of HTTP Requests ('HTTP Request Smuggling')20-Jan-20238.8versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS.https://www. dell.com/supp ort/kbdoc/en us/0020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS.https://www. dell.com/supp ort/kbdoc/en us/0020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerabilityProduct: reversult_me5/084versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desynchronize its connection with the website, typically leading to XSS and DoS.https://www. dell.com/supp outpate-for-a- client-desync- attack- vulnerabilityProduct: reversult_me5/084versions ME5.1.0.1.0, contains a Client-desync- attack- vulnerabilityhttps://www. dell.com/supp outpate-for-a- client-desync- attack- vulnerability	Affected Ver	sion(s): -				
-	Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023-	dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack-	POWE-
Affected Version(s): -	Product: po	wervault_me5	084			
	Affected Ver	sion(s): -				

0-1

1-2

2-3

3-44-5Page 358 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023- 23691	https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerability	H-DEL- POWE- 020223/535
Vendor: Om	iron				
Product: cp					
Affected Ver	sion(s): -			1	
N/A	17-Jan-2023	9.8	Active debug code exists in OMRON CP1L- EL20DR-D all versions, which may lead to a command that is not specified in FINS protocol being executed without authentication. A remote unauthenticated attacker may read/write in arbitrary area of the device memory, which may lead to overwriting the firmware, causing a denial-of-service (DoS) condition, and/or arbitrary code execution. CVE ID : CVE-2023- 22357	N/A	H-OMR- CP1L- 020223/536

0-1

1-2

 2-3
 3-4
 4-5

 Page 359 of 463

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cx-	motion-mch		L	L	
Affected Vers	sion(s): -				
Access of Uninitialize d Pointer	17-Jan-2023	7.8	CX-Motion-MCH v2.32 and earlier contains an access of uninitialized pointer vulnerability. Having a user to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution. CVE ID : CVE-2023- 22366	N/A	H-OMR-CX- M- 020223/537
Vendor: pix	ela				
Product: pix	x-rt100				
Affected Vers	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	8	OS command injection vulnerability in PIX- RT100 versions RT100_TEQ_2.1.1_EQ10 1 and RT100_TEQ_2.1.2_EQ10 1 allows a network- adjacent attacker who can access product settings to execute an arbitrary OS command. CVE ID : CVE-2023- 22304	https://www. pixela.co.jp/p roducts/netw ork/pix_rt100 /update.html	H-PIX-PIX 020223/538
N/A	17-Jan-2023	6.5	Hidden functionality vulnerability in PIX- RT100 versions RT100_TEQ_2.1.1_EQ10 1 and RT100_TEQ_2.1.2_EQ10 1 allows a network- adjacent attacker to access the product via undocumented Telnet or SSH services.	https://www. pixela.co.jp/p roducts/netw ork/pix_rt100 /update.html	H-PIX-PIX 020223/539

0-1

1-2

 2-3
 3-4
 4-5

 Page 360 of 463

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2023- 22316						
Vendor: Sor	Vendor: Sonicwall								
Product: sm	na1000								
Affected Ver	sion(s): -								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-2023	7.5	Pre-authentication path traversal vulnerability in SMA1000 firmware version 12.4.2, which allows an unauthenticated attacker to access arbitrary files and directories stored outside the web root directory. CVE ID : CVE-2023- 0126	https://psirt.g lobal.sonicwal l.com/vuln- detail/SNWLI D-2023-0001	H-SON- SMA1- 020223/540				
Vendor: Ter	nda			<u> </u>					
Product: ac									
Affected Ver									
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_000c231 8. CVE ID : CVE-2023- 24164	N/A	H-TEN-AC18- 020223/541				
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/initIpAddrInfo CVE ID : CVE-2023- 24165	N/A	H-TEN-AC18- 020223/542				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/formWifiBasic Set.	N/A	H-TEN-AC18- 020223/543	
			CVE ID : CVE-2023- 24166			
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/add_white_no de. CVE ID : CVE-2023- 24167	N/A	H-TEN-AC18- 020223/544	
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_0007343 c. CVE ID : CVE-2023- 24169	N/A	H-TEN-AC18- 020223/545	
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/fromSetWirel essRepeat. CVE ID : CVE-2023- 24170	N/A	H-TEN-AC18- 020223/546	
Vendor: Tp	-link		24170			
Product: tl-sg105pe						
Affected Version(s): 1.0						
Improper Authentica tion	17-Jan-2023	9.8	TP-Link SG105PE firmware prior to 'TL- SG105PE(UN) 1.0_1.0.0 Build 20221208' contains an	https://www. tp- link.com/jp/s upport/downl oad/tl-	H-TPTL-S- 020223/547	

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4
 4-5
 5-6
 6-7
 7-8
 8-9
 9-10

 Page 362 of 463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			authentication bypass vulnerability. Under the certain conditions, an attacker may impersonate an administrator of the product. As a result, information may be obtained and/or the product's settings may be altered with the privilege of the administrator. CVE ID : CVE-2023-	sg105pe/v1/ #Firmware, https://www. tp- link.com/en/ business- networking/e asy-smart- switch/tl- sg105pe/					
Vondor: Tro	ndnot		22303						
	Vendor: Trendnet Product: tew-820ap								
Affected Ver									
Out-of- bounds Write	23-Jan-2023	8.8	<pre>** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSystemCheck. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24095</pre>	N/A	H-TRE-TEW 020223/548				

0-1

1-2

2-3

3-4 4-5 Page **363** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	23-Jan-2023	8.8	 ** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the newpass parameter at /formPasswordSetup. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24096 	N/A	H-TRE-TEW 020223/549
Out-of- bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formPasswordAuth. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24097	N/A	H-TRE-TEW 020223/550

0-1

1-2

5-6

6-7 7-8 8-9

			** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-		
Out-of- bounds Write	23-Jan-2023	8.8	820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSysLog. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24098	N/A	H-TRE-TEW 020223/551
Out-of- bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the username parameter at /formWizardPassword. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24099	N/A	H-TRE-TEW 020223/552

0-1

1-2

 2-3
 3-4
 4-5

 Page 365 of 463

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Vendor: Ap	ple	I			<u>I</u>			
Product: macos								
Affected Ver	sion(s): -							
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21579	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/553			
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/554			

0-1

1-2

2-3

3-4 4-5 Page **366** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21604		
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21605	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/555
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21606	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/556

0-1

1-2

 2-3
 3-4
 4-5

 Page 367 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21607	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/557
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21608	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/558
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx. adobe.com/se curity/produc	O-APP- MACO- 030223/559

0-1

1-2

2-3

3-4 4-5 Page **368** of **463** 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609	ts/acrobat/ap sb23-01.html	
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/560
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/561

0-1

1-2

 2-3
 3-4
 4-5

 Page 369 of 463

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-		
			21611 Adobe Acrobat Reader		
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21612	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/562
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/563

0-1

1-2

2-3

3-4 4-5 Page **370** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21581		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21585	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/564
Use After Free	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage	https://helpx. adobe.com/se curity/produc ts/dimension /apsb23- 10.html	O-APP- MACO- 030223/565

0-1

1-2

2-33-44-5Page 371 of 463

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21601		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/dimension /apsb23- 10.html	O-APP- MACO- 030223/566
Out-of- bounds Read	18-Jan-2023	5.5	21603 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/567

0-1

1-2

2-3

3-4 4-5 Page **372** of **463** 7-8

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. CVE ID : CVE-2023- 21613		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21614	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-APP- MACO- 030223/568
Vendor: ate	-mahoroba				
Product: ma	aho-pbx_netde	vancer_fi	rmware		
Affected Ver	sion(s): * Up to	(excluding	g) 1.11.00		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/569

0-1

1-2

2-33-44-5Page 373 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute an arbitrary OS command. CVE ID : CVE-2023-		
			22279		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO- PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. CVE ID : CVE-2023- 22286	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/570
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/571

0-1

1-2

2-3

3-4 4-5 Page **374** of **463** 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. CVE ID : CVE-2023- 22280		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVE ID : CVE-2023- 22296	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/572
	-		obilegate_firmware		
Affected Ver	sion(s): * Up to	(excluding	g) 1.11.00		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command.	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/573

0-1

1-2

2-33-44-5Page 375 of 463

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22279		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO- PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. CVE ID : CVE-2023- 22286	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/574
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command.	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/575

0-1

1-2

2-3

3-4 4-5 Page **376** of **463** 5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22280		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVE ID : CVE-2023- 22296	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/576
Product: ma	aho-pbx_netde	vancer_v	sg_firmware		
Affected Ver	sion(s): * Up to	(excluding	g) 1.11.00		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command. CVE ID : CVE-2023- 22279	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/577

0-1

1-2

 2-3
 3-4
 4-5

 Page 377 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO- PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. CVE ID : CVE-2023- 22286	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/578
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. CVE ID : CVE-2023- 22280	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/579

0-1

1-2

2-3

3-4 4-5 Page **378** of **463** 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO- PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. CVE ID : CVE-2023- 22296	https://www. ate- mahoroba.jp/ netdevancer/ manual/	O-ATE- MAHO- 030223/580
Vendor: Cis	со			I	I
Product: as					
Affected Ver	sion(s): -			1	
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-esa- url-bypass- WbMQqNJh	0-CIS-ASYN- 030223/581

0-1

1-2

 2-3
 3-4
 4-5

 Page 379 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Des	cription & C	VE ID	Pato	:h	NCII	PC ID
			exploit attacko URL re that ar an affe which malicio	successfu t could allo er to bypa eputation f ce configur ected devic could allo ous URLs t gh the devi	ow the ss the ilters ed for e, w o pass				
			CVE II 20057	D : CVE-20	23-				
Product: ip_	phones_8832_	firmware	e						
Affected Ver	sion(s): * Up to	(excludin	g) 14.1\	\(1\\)sr2					
Incorrect Authorizati on	20-Jan-2023	6.5	web-ba manag of Cisc and 88 could a unauth remote bypass on an a This vu to insu validat supplic attacke this vu sendin reques based interfa exploit attacke certair interfa auther	gement int to IP Phone 300 Series allow an henticated e attacker s authentic affected de ulnerabilit ifficient tion of use ed input. <i>A</i> er could es ilnerability of a crafted st to the w management ace. A succe t could allo er to access n parts of t ace that wo ully require ntication. D : CVE-20	erface 2 7800 Phones to cation evice. y is due r- an cploit y by l eb- ent essful ow the s he web ould e	https:// oudapps .com/see /center/ nt/Cisco ityAdvis sco-sa-ip phone-a bypass- pSqxZRF	s.cisco curity /conte oSecur ory/ci o- uth-	0-CIS- 03022	_
riouuci: ip_	_phone_7800_f	ninware							
CVSS Scoring S	Scale 0-1	1-2 2	2-3 3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Page 380 of 463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/583
-	phone_7811_f				
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/584

0-1

1-2

 2-3
 3-4
 4-5

 Page 381 of 463

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.		
			CVE ID : CVE-2023- 20018		
-	phone_7821_f				
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/585

0-1

1-2

2-3

3-4 4-5 Page **382** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			normally require authentication.			
			CVE ID : CVE-2023- 20018			
Product: ip_	phone_7832_f	irmware				
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2			
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/586	
Product: ip_phone_7841_firmware Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2						
Allected ver		excluding	g) 14.1\\(1\\)sr2	https://sec.cl		
Incorrect Authorizati on	20-Jan-2023	6.5	web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-IP_P- 030223/587	

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	
Product: ip_	phone_7861_f	irmware	20010		
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/588

0-1

1-2

2-3

3-4 4-5 Page **384** of **463** 5-6

Incorrect Authorizati on20-Jan-20236.56.5A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018https://sec.cl oudalps.cisco could allow the attacker could exploit on an affected device. This vulnerability is due to insufficient validation of user- sending a cafted request to the web- based management interface that would normally require authentication.https://sec.cl oudalps.cisco could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a cafted request to the web- based management interface that would normally require authentication. CVE ID : CVE-2023- 20018https://sec.cl oudapps.cisco com/security /center/conte nt/CiscoSecur phone-auth- bypass sending a cafted request to the web- based management interface that would normally require authentication. CVE ID : CVE-2023- 20018https://sec.cl outalpps.cisco com/security co-sa-ip- phone-auth- bypass pho	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization20-Jan-20236.56.5A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to b bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web- based management interface that would normally require authentication.https://sec.cl oudapps.cisco .com/security /center/conter ityAdvisory/ci g030223/589 phone-auth- bypass- pSqxZRPR0-CIS-IP_P- 030223/589				interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.		
Affected Version(s): * Up to (excluding) 14.1\\(1\)sr2Affected Version(s): * Up to (excluding) 14.1\\(1\)sr2A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management 						
Incorrect Authorizati on20-Jan-20236.5A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficienthttps://sec.cl oudapps.cisco oudapps.cisco ityAdvisory/ci 030223/58920-Jan-20236.56.5Https://sec.cl oudapps.cisco this vulnerability by sending a crafted request to the web- based management interface that would normally require authentication.0-CIS-IP_P- 030223/589CVE ID : CVE-2023- 20018CVE ID : CVE-2023- 200180-CIS-IP_P- 030223/589	Product: ip_	phone_8800_f	irmware			
Incorrect Authorizati on20-Jan-20236.5essentiation onweb-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface that would normally require authentication.https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur 030223/589O-CIS-IP_P- 030223/5890-CIS-IP_P- 030223/589	Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
	Authorizati on			web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass-	—
	Product: ip	phone_8811_f	irmware			

0-1

1-2

2-3

3-4 4-5 Page **385** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/590
Product: ip_	phone_8821-e	x_firmwa	ire		
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/591

0-1

1-2

 2-3
 3-4
 4-5

 Page 386 of 463

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.		
			CVE ID : CVE-2023- 20018		
Product: ip_phone_8821_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/592

0-1

1-2

2-3

3-4 4-5 Page **387** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			normally require authentication.						
			CVE ID : CVE-2023- 20018						
Product: ip_	Product: ip_phone_8831_firmware								
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2						
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	0-CIS-IP_P- 030223/593				
-	phone_8832_f		(1) 14 1 (1) (1) 0 000						
Incorrect Authorizati on	20-Jan-2023	6.5	g) 14.1\\(1\\)sr2 A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur	O-CIS-IP_P- 030223/594				

2-3 3-4 4-5 Page 388 of 463

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	
Product: ip_	phone_8841_f	irmware	20010		
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/595

0-1

1-2

2-3

3-4 4-5 Page **389** of **463** 8-9

9-10

6-7

roduct: ip_phone_8845_firmware fected Version(s): * Up to (excluding) 14.1\\(1\\)sr2 A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated,	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coduct: ip_phone_8845_firmware 20018 ifected Version(s): * Up to (excluding) 14.1\\(1\\)sr2 A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an				interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.		
Fected Version(s): * Up to (excluding) 14.1\\(1\\)sr2 A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an						
A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an	Product: ip	phone_8845_f	irmware			
web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an	Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Ithorizati20-Jan-20236.5supplied input. All attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication.nt/CiscoSecur ityAdvisory/ci 030223/596030223/596 ityAdvisory/ci030223/596 sco-sa-ip- phone-auth- bypass- pSqxZRPR	Incorrect Authorizati on			web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-	oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass-	O-CIS-IP_P- 030223/596
roduct: ip_phone_8851_firmware	Product: ip	phone_8851_f	irmware			

0-1

1-2

2-3

3-4 4-5 Page **390** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2							
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/597			
Product: ip_	_phone_8861_f	irmware						
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2					
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/598			

0-1

1-2

2-33-44-5Page **391** of **463**

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018		
Product: ip	phone_8865_f	irmware	20010		
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-IP_P- 030223/599

0-1

1-2

2-3

3-4 4-5 Page **392** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			normally require authentication. CVE ID : CVE-2023- 20018					
Product: ro	omos							
Affected Version(s): 10.11.3.0								
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/600			
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	O-CIS-ROOM- 030223/601			

0-1

1-2

2-3

3-4 4-5 Page **393** of **463** 5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.		
			CVE ID : CVE-2023- 20002		
Affected Ver	sion(s): 10.11.5	.2	L		
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/602

0-1

1-2

2-3

3-4 4-5 Page **394** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	O-CIS-ROOM- 030223/603
Affected Ver	sion(s): 10.15.3	.0			
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/604

0-1

1-2

 2-3
 3-4
 4-5

 Page 395 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/605
Affected Ver	sion(s): 10.3.2.0)			
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-	0-CIS-ROOM- 030223/606

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	roomos- dkjGFgRK	
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/607

0-1

1-2

2-3

3-4 4-5 Page **397** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2023- 20002						
Affected Ver	Affected Version(s): 10.3.4.0								
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/608				
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/609				

0-1

1-2

 2-3
 3-4
 4-5

 Page 398 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023-		
			20002		
Affected Ver	sion(s): 10.8.2.5	5			
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. CVE ID : CVE-2023- 20008	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/610
Server- Side Request	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cl oudapps.cisco .com/security /center/conte	0-CIS-ROOM- 030223/611

0-1

1-2

2-3 3-4 4-5 Page **399** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023-	nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	
			20002		
Affected Ver	sion(s): 10.8.4.0)			
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/612

0-1

1-2

 2-3
 3-4
 4-5

 Page 400 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to overwrite arbitrary files on the affected device.		
			CVE ID : CVE-2023- 20008		
Server- Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. CVE ID : CVE-2023- 20002	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- roomos- dkjGFgRK	0-CIS-ROOM- 030223/613
Product: rv	016_firmware				
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device.	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	0-CIS-RV01- 030223/614

0-1

1-2

2-3

3-4 4-5 Page **401** of **463** 5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025		
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	0-CIS-RV01- 030223/615

0-1

1-2

2-33-44-5Page 402 of 463

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device.		
			CVE ID : CVE-2023- 20026		
Product: rv	042g_firmware	è			
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	O-CIS-RV04- 030223/616
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci	O-CIS-RV04- 030223/617

0-1

1-2

 2-3
 3-4
 4-5

 Page 403 of 463

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. CVE ID : CVE-2023- 20026	sco-sa- sbr042-multi- vuln- ej76Pke5	
	042_firmware				
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	0-CIS-RV04- 030223/618
CV/SS Scoring S		1_2		6.7 7.9	8.0 0.10
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 404 of 463	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025		
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	0-CIS-RV04- 030223/619

0-1

1-2

2-33-44-5Page 405 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have valid Administrator credentials on the affected device.		
			CVE ID : CVE-2023- 20026		
Product: rv	082_firmware				
Affected Ver	sion(s): -				
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web- based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. CVE ID : CVE-2023- 20025	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi- vuln- ej76Pke5	O-CIS-RV08- 030223/620
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa- sbr042-multi-	O-CIS-RV08- 030223/621

0-1

1-2

 2-3
 3-4
 4-5

 Page 406 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. CVE ID : CVE-2023- 20026	vuln- ej76Pke5	
Product: rv	160w_wireless	-ac_vpn_i	router_firmware		
Affected Ver	sion(s): * Up to	(excluding	g) 1.0.01.04		
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-rv- cmd-exe- n47kJQLE	O-CIS-RV16- 030223/622

0-1

1-2

2-3

3-4 4-5 Page **407** of **463** 5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator- level credentials on the affected device. CVE ID : CVE-2023-		
			20045		
	160_vpn_route				
Affected ver	sion(s): * Up to	(excluding			
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-rv- cmd-exe- n47kJQLE	0-CIS-RV16- 030223/623

0-1

1-2

2-3

3-4 4-5 Page **408** of **463** 6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to the web- based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator- level credentials on the affected device.		
			CVE ID : CVE-2023- 20045		
	260p_vpn_rout	-	•		
Affected Ver	sion(s): * Up to	(excluding			
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface of an affected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-rv- cmd-exe- n47kJQLE	O-CIS-RV26- 030223/624

0-1

1-2

2-3

3-4 4-5 Page **409** of **463** 5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator- level credentials on the affected device. CVE ID : CVE-2023-		
Due de et ere	260	- C	20045		
	260_vpn_route sion(s): * Up to				
Allected ver	sion(s): • op to	(excluding			
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-rv- cmd-exe- n47kJQLE	0-CIS-RV26- 030223/625

0-1

1-2

2-3

3-4 4-5 Page **410** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator- level credentials on the affected device. CVE ID : CVE-2023- 20045		
Product: rv	<mark>340w_firmwar</mark>	е			
	- rsion(s): * Up to		g) 1.0.03.29		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos- 7HjP74jD	0-CIS-RV34- 030223/626

0-1

1-2

2-3

3-4 4-5 Page **411** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. CVE ID : CVE-2023-		
			20007		
	340_firmware		.) 1 0 02 20		
Affected ver	sion(s): * Up to	cexcluding			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos- 7HjP74jD	0-CIS-RV34- 030223/627

0-1

1-2

2-3

3-4 4-5 Page **412** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. CVE ID : CVE-2023-		
			20007		
	345p_firmwar				
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos- 7HjP74jD	O-CIS-RV34- 030223/628

0-1

1-2

2-3

3-4 4-5 Page **413** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. CVE ID : CVE-2023- 20007		
Product: rv	345_firmware		20007		
	sion(s): * Up to	(excluding	g) 1.0.03.29		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-sb-rv- rcedos- 7HjP74jD	0-CIS-RV34- 030223/629

0-1

1-2

2-3

3-4 4-5 Page **414** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition.		
			CVE ID : CVE-2023- 20007		
	ified_ip_phone				
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2	I	
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	0-CIS-UNIF- 030223/630

0-1

1-2

2-3

3-4 4-5 Page **415** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			certain parts of the web interface that would normally require authentication.			
			CVE ID : CVE-2023- 20018			
Product: un	ified_ip_phone	_8865nr_	firmware			
Affected Ver	sion(s): * Up to	(excluding	g) 14.1\\(1\\)sr2			
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	O-CIS-UNIF- 030223/631	
-	Product: webex_room_phone_firmware Affected Version(s): * Up to (including) 1.2.0					
	sion(s): * Up to	(including		1		
Allocation of Resources	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature	https://sec.cl oudapps.cisco .com/security	O-CIS-WEBE- 030223/632	

0-1

1-2

2-3

3-4 Page **416** of **463**

4-5

5-6

6-7

Without Limits or of Cisco Webex Room /center/conte Throttling Phone and Cisco Webex nt/CiscoSecurity Allocation adjacent attacker to sco-sa-lldp- unauthenticated, memik- McOecPT Custo a denial of service (DoS) condition on an affected device. This wulnerability is due to unauthenticated, unauthenticated, memik- McOecPT allocation. An attacker could exploit this wulnerability by sending crafted LLDP traffic to an affected device, device, Astacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support buspert bot Gisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- condaty Allocation 20-Jan-2023 6.5 A vulnerability in the htttps://sec.cl	Weakness	Publish Date	CVSSv3	Descript	ion & CVE	ID	Pato	ch	NCII	PC ID
Product: webex_share_firtwareexploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047image: CVE ID : CVE-2023- 20047Allocation of cf20-Jan-20236.5A vulnerability in the Link Layer Discovery Protocol (LLDP) featurehttps://sec.cl oudapps.cisco oudapps.cisco com/security0-CIS-WEBE- 030223/633	Without Limits or	Publish Date	CVSSv3	of Cisco W Phone and Share devi allow an unauthent adjacent a cause a de (DoS) cone affected de vulnerabil insufficien allocation. could expl vulnerabil sending cr traffic to a	ebex Roc l Cisco W ices could icated, ttacker to nial of se dition on evice. Thi ity is due t resourc An attac oit this ity by afted LLI n affected	om ebex d rvice an s to ce ker	/center/ nt/Cisco ityAdvis sco-sa-ll memlk-	/conte Secur ory/ci dp-	NCII	PC ID
to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047Image: CVE ID image: CVE-2023- 20047Product: wex_share_fir/wareAffected Version(s): * Up to (including) 1.2.0Allocation of of Resources20-Jan-20236.5A vulnerability in the Link Layer Discovery Protocol (LLDP) featurehttps://sec.cl oudapps.cisco .com/security0-CIS-WEBE- 030223/633CVSS Scoring Scale0-11-22-33-44-55-66-77-88-9910				device. A s exploit cou attacker to memory re the affecte resulting i the LLDP p affected de configured LLDP only cause an in inbound a calling. By	euccessful ald allow o exhaust esources ed device, n a crash process. I evice is l to suppo to suppo this cou nterruption default, t	l the of of f the ort ld on to und these				
Product: webex_share_fir ware Affected Version(s): * Up to (including) 1.2.0 Allocation of a sources 20-Jan-2023 6.5 A vulnerability in the Link Layer Discovery Protocol (LLDP) feature https://sec.cl oudapps.cisco oudapps.cisco oudapps.cisco 0-CIS-WEBE-030223/633 CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				to support Discovery LLDP. To r operationa affected de manual re CVE ID : C	both Cis Protocol recover al state, tl evice nee start.	co and he ds a				
Affected Version(s): * Up to (including) 1.2.0 Allocation of of Resources 20-Jan-2023 6.5 A vulnerability in the Link Layer Discovery Protocol (LLDP) feature https://sec.cl oudapps.cisco oudapps.cisco com/security 0-CIS-WEBE-030223/633 CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Product: we	bex share firr	nware	20047						
Allocation of of Resources 20-Jan-2023 6.5 A vulnerability in the Link Layer Discovery Protocol (LLDP) feature https://sec.cl oudapps.cisco oudapps.cisco i.com/security 0-CIS-WEBE-030223/633 CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				v) 1 2 0						
	Allocation of			A vulneral Link Layer	Discove	ry	oudapps	s.cisco		
	CVSS Scoring S	Scale 0-1	1-2 2			5-6	6-7	7-8	8-9	9-10

Without inits or of Cisco Webex Room //center/conte Imits or Phone and Cisco Webex nt/CiscoSecur Throttling allow an sco-sa-Ildp- unauthenticated, adjacent attacker to cause a denial of service (DS) condition on an affected device. This wulnerability is due to unsufficient resource allocation. An attacker memilk- could exploit this vulnerability sending crafted LDP trafficted device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device is configured to support LDP poly, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LDP. To recover operational state, the affected device needs a manual restart. CVEI D: CVE-2023-2 Z0047 CVEI D: CVE-2023-2 20047	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Throttling Share devices could iiyAdvisory/ci allow an sco-sa-ldp- memlk- adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LDP process. If the affected device, resulting in a crash of the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047	Without			of Cisco Webex Room	/center/conte					
allow ansco-sa-Ildp- memIk- McOecPTadjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP proly, this could cause a initerruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wireless.ip_phote_t8821-ex_firmware	Limits or			Phone and Cisco Webex	nt/CiscoSecur					
unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. Product: wireless. ip_phous_8821-ex_tirmware	Throttling			Share devices could	ityAdvisory/ci					
McOecPTcause a denial of service (DOS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device is configured to support LDP process. If the affected device is configured to support toto insound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.McOecPTProduct: wtwetess.ip_thouse.test.test.test.testVUInerability by sending restart.McOecPTProduct: wtwetess.ip_thouse.test.test.test.test.testMcOecPT					•					
cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047				unauthenticated,						
(DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both CIsco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023-20047		adjacent attacker to McOecPT								
affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047										
vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the attacker to exhaust the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.vulnerability is due to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.vulnerability is due to inbound and eveloal a could allow the could affected device needs a manual restart.Product: wireless_ip_bnote_8821-tsvulnerability is due to informationvulnerability is due to information could allow the affected device needs a manual restart.		(DoS) condition on an								
Product: wireless_ip_phone_8821-ex_tirmware insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047 zover				affected device. This						
Product: wireless_ip_photeallocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wireless_ip_ptore_8821-vects/fitUCK-2023- 20047				vulnerability is due to						
Product: wrueless_ip_phone_882tcould exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wrueless_ip_phone_882t=vt=wt=				insufficient resource						
Vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wireless_ip_phone_8821-ex_tirmware				allocation. An attacker						
Product: wireless_ip_phone_8821-ex_firedsending crafted LLDPtraffic to an affecteddevice. A successfulexploit could allow theattacker to exhaust thememory resources ofthe affected device,resulting in a crash ofthe LLDP process. If theaffected device isconfigured to supportLLDP only, this couldcause an interruption toinbound and outboundcalling. By default, thesedevices are configuredto support both CiscoDiscovery Protocol andLLDP. To recoveroperational state, theaffected device needs amanual restart.CVE ID: CVE-2023-20047				could exploit this						
Product: wireless.jp_phote_8821-w_firmwaretraffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wireless.ip_phone_8821-w_firmware				vulnerability by						
Product: wireless.jp_phote_8821device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Here affected device needs a manual restart.VEVE ID : CVE-2023- 20047CVE ID : CVE-2023- 20047Here affected device needs a manual restart.				sending crafted LLDP						
Product: wireless_ip_browexploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.CVE ID : CVE-2023- 20047CVE ID : CVE-2023- 20047				traffic to an affected						
attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wireless_ip_phone_8821-wure				device. A successful						
Product: wireless_ip_phonememory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wireless_ip_phone_8821-wirelessCVE ID : CVE-2023- 20047				exploit could allow the						
Product:Image by the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.CVE ID : CVE-2023- 20047CVE ID : CVE-2023- 20047				attacker to exhaust the						
Product: wterse.jp.phone.set (a) and and outportIntersection (a) (b) (b) (b) (b) (b) (b) (b) (b) (b) (b				memory resources of						
the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.Product: wireless_ip_pho=table.the LLDP process. If the affected.the affected.				the affected device,						
Image: state s				resulting in a crash of						
Product: wireless_ip_phoneconfigured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart.CVE ID : CVE-2023- 20047Product: wireless_ip_phone_8821-exe				the LLDP process. If the						
LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047 Product: wireless_ip_phone_8821-ex_firmware				affected device is						
Image: state in the state in				configured to support						
Image: space s				LLDP only, this could						
Image: state in the state in				cause an interruption to						
devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047				inbound and outbound						
Product: wireless_ip_phone_8821-ex_firmware				calling. By default, these						
Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047 Product: wireless_ip_phone_8821-ex_firmware				devices are configured						
Image: LLDP. To recover operational state, the operational state, the affected device needs a manual restart. CVE ID : CVE-2023- 20047 20047				to support both Cisco						
Product: wireless_ip_phone_8821-ex_firmware operational state, the affected device needs a manual restart. CVE ID : CVE-2023-20047 count of the state of the				Discovery Protocol and						
affected device needs a manual restart. CVE ID : CVE-2023-20047 Product: wireless_ip_phone_8821-ex_firmware				LLDP. To recover						
manual restart. CVE ID : CVE-2023- 20047 20047				operational state, the						
Product: wireless_ip_phone_8821-ex_firmware				affected device needs a						
Product: wireless_ip_phone_8821-ex_firmware		manual restart.								
Product: wireless_ip_phone_8821-ex_firmware		CVE ID : CVE-2023-								
Affected Version(s): * Up to (excluding) 11.0\\(6\\)sr4	Product: wi	reless_ip_phon	e_8821-e	ex_firmware						
	Affected Ver	sion(s): * Up to	(excludin	g) 11.0\\(6\\)sr4						

0-1

1-2

2-33-44-5Page 418 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user- supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023- 20018	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	0-CIS-WIRE- 030223/634
	reless_ip_phor				
Affected Ver	sion(s): * Up to	(excludin	g) 11.0\\(6\\)sr4		
Incorrect Authorizati on	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-	https://sec.cl oudapps.cisco .com/security /center/conte nt/CiscoSecur ityAdvisory/ci sco-sa-ip- phone-auth- bypass- pSqxZRPR	0-CIS-WIRE- 030223/635

0-1

1-2

2-3

3-4 4-5 Page **419** of **463** 8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web- based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. CVE ID : CVE-2023-		
Vendor: Del	bian		20018		
Product: de	bian_linux				
Affected Ver	sion(s): 10.0				
N/A	20-Jan-2023	9.8	Incorrect handling of '\0' bytes in file uploads in ModSecurity before 2.9.7 may allow for Web Application Firewall bypasses and buffer overflows on the Web Application Firewall when executing rules that read the FILES_TMP_CONTENT collection. CVE ID : CVE-2023- 24021	https://githu b.com/Spider Labs/ModSec urity/pull/28 57/commits/ 4324f0ac59f8 225aa44bc50 34df60dbeccd 1d334, https://githu b.com/Spider Labs/ModSec urity/pull/28 57	O-DEB-DEBI- 030223/636
Improper Privilege Manageme nt	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local	https://www. sudo.ws/secu rity/advisorie s/sudoedit_an y/, https://securi ty.netapp.com /advisory/nta	O-DEB-DEBI- 030223/637

0-1

1-2

2-33-44-5Page 420 of 463

8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user- specified editor may contain a "" argument that defeats a protection mechanism, e.g., an EDITOR='vim /path/to/extra/file' value.	p-20230127- 0015/	
			CVE ID : CVE-2023- 22809		
Affected Ver	sion(s): 11.0		In Sudo before		
Improper Privilege Manageme nt	18-Jan-2023	7.8	1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user- specified editor may contain a "" argument that defeats a protection mechanism, e.g., an EDITOR='vim	https://www. sudo.ws/secu rity/advisorie s/sudoedit_an y/, https://securi ty.netapp.com /advisory/nta p-20230127- 0015/	O-DEB-DEBI- 030223/638

0-1

1-2

2-33-44-5Page 421 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/path/to/extra/file' value.		
			CVE ID : CVE-2023- 22809		
Vendor: De	1			1	
Product: po	wervault_me5	012_firm	ware		
Affected Ver	sion(s): * Up to	(excludin	g) me5.1.1.0.5	-	
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023- 23691	https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerability	O-DEL- POWE- 030223/639
-	wervault_me5				
Affected Ver	sion(s): * Up to	(excludin	g) me5.1.1.0.5		
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS.	https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerability	O-DEL- POWE- 030223/640

0-1

1-2

2-3

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23691		
-	wervault_me5				
Affected Ver	sion(s): * Up to	(excluding	g) me5.1.1.0.5		
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. CVE ID : CVE-2023- 23691	https://www. dell.com/supp ort/kbdoc/en - us/00020753 3/dsa-2023- 018-dell-emc- powervault- me5-security- update-for-a- client-desync- attack- vulnerability	O-DEL- POWE- 030223/641
Vendor: Fed	loraproject				
Product: fee	lora				
Affected Ver	sion(s): 37				
Improper Privilege Manageme nt	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists	https://www. sudo.ws/secu rity/advisorie s/sudoedit_an y/, https://securi ty.netapp.com /advisory/nta p-20230127- 0015/	O-FED-FEDO- 030223/642

0-1

1-2

2-33-44-5Page 423 of 463

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because a user- specified editor may contain a "" argument that defeats a protection mechanism, e.g., an EDITOR='vim /path/to/extra/file' value.		
			CVE ID : CVE-2023- 22809		
Vendor: Go	ogle				
Product: an					
Affected Ver	sion(s): -				
Use After Free	26-Jan-2023	7.8	In setUclampMinLocked of PowerSessionManager. cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 236674672References: N/A CVE ID : CVE-2023- 20925	https://sourc e.android.com /security/bull etin/pixel/20 23-01-01	0-GOO- ANDR- 030223/643
Use After Free	26-Jan-2023	7.8	In binder_vma_close of binder.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/644

0-1

1-2

2-3

3-4 4-5 Page **424** of **463** 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 254837884References: Upstream kernel CVE ID : CVE-2023- 20928		
Improper Authentica tion	26-Jan-2023	6.8	In (TBD) of (TBD), there is a possible way to bypass the lockscreen due to Biometric Auth Failure. This could lead to local escalation of privilege with physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 240428519References: N/A CVE ID : CVE-2023- 20924	https://sourc e.android.com /security/bull etin/pixel/20 23-01-01	0-GOO- ANDR- 030223/645
N/A	26-Jan-2023	5.5	In exported content providers of ShannonRcs, there is a possible way to get access to protected content providers due to a permissions bypass. This could lead to local information disclosure with no additional execution	https://sourc e.android.com /security/bull etin/pixel/20 23-01-01	0-G00- ANDR- 030223/646

0-1

1-2

2-3

3-4 4-5 Page **425** of **463** 6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 246933910References: N/A CVE ID : CVE-2023- 20923		
Affected Ver	sion(s): 10.0				
Out-of- bounds Write	26-Jan-2023	7.8	In Mfc_Transceive of phNxpExtns_MifareStd. cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-241387741 CVE ID : CVE-2023- 20905	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/647
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.8	In addOrReplacePhoneAcc ount of PhoneAccountRegistrar .java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. This could lead to local escalation of privilege with no additional	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/648

0-1

1-2

2-3

3-4 4-5 Page **426** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 246930197 CVE ID : CVE-2023- 20915		
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 204584366 CVE ID : CVE-2023-	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/649
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.3	20920 In onPackageRemoved of AccessibilityManagerSe rvice.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/650

0-1

1-2

2-3

3-4 4-5 Page **427** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 243378132 CVE ID : CVE-2023- 20921		
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 239415861	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/651
Affected Ver	ation (a): 11 0		CVE ID : CVE-2023- 20908		
	sion(s): 11.0				
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.8	In addOrReplacePhoneAcc ount of PhoneAccountRegistrar .java, there is a possible way to enable a phone	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/652

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account without user interaction due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 246930197		
			CVE ID : CVE-2023- 20915		
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 204584366 CVE ID : CVE-2023- 20920	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/653

0-1

1-2

2-3

3-4 4-5 Page **429** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerSe rvice.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 13Android ID: A- 243378132 CVE ID : CVE-2023- 20921	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/654
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 239415861	https://sourc e.android.com /security/bull etin/2023-01- 01	O-GOO- ANDR- 030223/655

0-1

1-2

 2-3
 3-4
 4-5

 Page
 430 of
 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 20908		
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In setMimeGroup of PackageManagerServic e.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A- 237291548 CVE ID : CVE-2023- 20922	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/656
Affected Ver	sion(s): 12.0				
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.8	In addOrReplacePhoneAcc ount of PhoneAccountRegistrar .java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/657

0-1

1-2

 2-3
 3-4
 4-5

 Page 431 of 463

5-6

6-7

7-8 8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A- 246930197 CVE ID : CVE-2023- 20915		
Missing Authorizati on	26-Jan-2023	7.8	In getMainActivityLaunchI ntent of LauncherAppsService.ja va, there is a possible way to bypass the restrictions on starting activities from the background due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12LAndroid ID: A- 229256049 CVE ID : CVE-2023- 20916	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/658
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/659

0-1

1-2

2-3

3-4 4-5 Page **432** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android- 12L Android- 13Android ID: A- 204584366		
			CVE ID : CVE-2023- 20920		
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerSe rvice.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 13Android ID: A- 243378132 CVE ID : CVE-2023- 20921	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/660
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/661

0-1

1-2

2-3

3-4 4-5 Page **433** of **463** 8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 239415861		
			CVE ID : CVE-2023- 20908		
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In setMimeGroup of PackageManagerServic e.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A- 237291548	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/662
			CVE ID : CVE-2023- 20922		
Affected Ver	sion(s): 12.1		I		
N/A	26-Jan-2023	7.8	In getTrampolineIntent of SettingsActivity.java, there is a possible launch of arbitrary activity due to an Intent mismatch in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/663

0-1

1-2

2-3

3-4 4-5 Page **434** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12L Android- 13Android ID: A- 246300272		
			CVE ID : CVE-2023- 20904		
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.8	In addOrReplacePhoneAcc ount of PhoneAccountRegistrar .java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 246930197 CVE ID : CVE-2023-	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/664
			20915		
Missing Authorizati on	26-Jan-2023	7.8	In getMainActivityLaunchI ntent of LauncherAppsService.ja va, there is a possible way to bypass the restrictions on starting activities from the background due to a missing permission check. This could lead to local escalation of privilege with no	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/665

0-1

1-2

2-3

3-4 4-5 Page **435** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android- 12LAndroid ID: A- 229256049 CVE ID : CVE-2023- 20916		
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 204584366 CVE ID : CVE-2023- 20920	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/666
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerSe rvice.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/667

0-1

1-2

2-3

3-4 4-5 Page **436** of **463** 5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 243378132 CVE ID : CVE-2023- 20921		
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 239415861 CVE ID : CVE-2023-	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/668
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	20908 In setMimeGroup of PackageManagerServic e.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/669

0-1

1-2

2-3

3-4 4-5 Page **437** of **463** 5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A- 237291548		
			CVE ID : CVE-2023- 20922		
Affected Ver	sion(s): 13.0		·		
N/A	26-Jan-2023	7.8	In getTrampolineIntent of SettingsActivity.java, there is a possible launch of arbitrary activity due to an Intent mismatch in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android- 13Android ID: A- 246300272 CVE ID : CVE-2023- 20904	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/670
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.8	In addOrReplacePhoneAcc ount of PhoneAccountRegistrar .java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. This could lead to local escalation of privilege with no additional	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/671

0-1

1-2

2-3

3-4 4-5 Page **438** of **463** 6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 246930197 CVE ID : CVE-2023- 20915		
N/A	26-Jan-2023	7.8	In getStringsForPrefix of Settings.java, there is a possible prevention of package uninstallation due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-252663068 CVE ID : CVE-2023-	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/672
Use After Free	26-Jan-2023	7.8	20919 In queue of UsbRequest.java, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/673

0-1

1-2

 2-3
 3-4
 4-5

 Page 439 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 204584366		
			CVE ID : CVE-2023- 20920		
Always- Incorrect Control Flow Implement ation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerSe rvice.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 243378132 CVE ID : CVE-2023- 20921	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/674
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not	https://sourc e.android.com /security/bull etin/2023-01- 01	0-G00- ANDR- 030223/675

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android- 12L Android- 13Android ID: A- 239415861		
			CVE ID : CVE-2023- 20908		
Uncontroll ed Resource Consumpti on	26-Jan-2023	5.5	In setMimeGroup of PackageManagerServic e.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A- 237291548 CVE ID : CVE-2023- 20922	https://sourc e.android.com /security/bull etin/2023-01- 01	0-GOO- ANDR- 030223/676
Vendor: Lin	ux				
Product: lin	_				
Affected Ver	sion(s): -				
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	17-Jan-2023	7.5	IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that	https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244356, https://www. ibm.com/sup port/pages/n ode/6855643	0-LIN-LINU- 030223/677

0-1

1-2

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key. IBM X-Force ID: 244356. CVE ID : CVE-2023- 22875		
Affected Ver	sion(s): * Up to	(excluding	g) 6.1		
Use After Free	26-Jan-2023	5.5	A use-after-free flaw was found in io_uring/filetable.c in io_install_fixed_file in the io_uring subcomponent in the Linux Kernel during call cleanup. This flaw may lead to a denial of service. CVE ID : CVE-2023-	https://bugzil la.redhat.com /show_bug.cgi ?id=2163723	0-LIN-LINU- 030223/678
			0469		
Use After Free	26-Jan-2023	4.7	A use-after-free flaw was found in io_uring/poll.c in io_poll_check_events in the io_uring subcomponent in the Linux Kernel due to a race condition of poll_refs. This flaw may cause a NULL pointer dereference. CVE ID : CVE-2023-	https://bugzil la.redhat.com /show_bug.cgi ?id=2164024	0-LIN-LINU- 030223/679
			0468		
Affected Ver	sion(s): * Up to	(excluding	g) 6.2	•	
NULL Pointer Dereferenc e	26-Jan-2023	5.5	A NULL pointer dereference flaw was found in rawv6_push_pending_fr ames in net/ipv6/raw.c in the network subcomponent in the Linux kernel. This flaw causes the system to crash.	https://git.ke rnel.org/pub/ scm/linux/ke rnel/git/torva lds/linux.git/c ommit/?id=cb 3e9864cdbe3 5ff637896666 0edbcbac955f e17	O-LIN-LINU- 030223/680

0-1

1-2

2-33-44-5Page 442 of 463

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0394		
Affected Ver	sion(s): 6.0				
NULL Pointer Dereferenc e	17-Jan-2023	7.5	A NULL pointer dereference vulnerability in the Linux kernel NVMe functionality, in nvmet_setup_auth(), allows an attacker to perform a Pre-Auth Denial of Service (DoS) attack on a remote machine. Affected versions v6.0-rc1 to v6.0-rc3, fixed in v6.0- rc4. CVE ID : CVE-2023-	https://git.ke rnel.org/pub/ scm/linux/ke rnel/git/torva lds/linux.git/c ommit/?id=da 0342a3aa035 7795224e628 3df86444e11 17168	0-LIN-LINU- 030223/681
			0122		
Affected Ver	sion(s): 6.1				
Use After Free	26-Jan-2023	5.5	A use-after-free flaw was found in io_uring/filetable.c in io_install_fixed_file in the io_uring subcomponent in the Linux Kernel during call cleanup. This flaw may lead to a denial of service.	https://bugzil la.redhat.com /show_bug.cgi ?id=2163723	O-LIN-LINU- 030223/682
			CVE ID : CVE-2023- 0469		
Use After Free	26-Jan-2023	4.7	A use-after-free flaw was found in io_uring/poll.c in io_poll_check_events in the io_uring subcomponent in the Linux Kernel due to a race condition of poll_refs. This flaw may	https://bugzil la.redhat.com /show_bug.cgi ?id=2164024	0-LIN-LINU- 030223/683

0-1

1-2

2-3

3-4 4-5 Page **443** of **463** 5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a NULL pointer dereference.		
			CVE ID : CVE-2023- 0468		
Affected Ver	sion(s): 6.2				
NULL Pointer Dereferenc e	26-Jan-2023	5.5	A NULL pointer dereference flaw was found in rawv6_push_pending_fr ames in net/ipv6/raw.c in the network subcomponent in the Linux kernel. This flaw causes the system to crash. CVE ID : CVE-2023- 0394	https://git.ke rnel.org/pub/ scm/linux/ke rnel/git/torva lds/linux.git/c ommit/?id=cb 3e9864cdbe3 5ff637896666 0edbcbac955f e17	0-LIN-LINU- 030223/684
Vendor: Mic	crosoft				
Product: wi	ndows				
Affected Ver	sion(s): -				
Integer Overflow or Wraparoun d	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21579	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/685

0-1

1-2

 2-3
 3-4
 4-5

 Page
 444 of
 463

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21604	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/686
Heap- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21605	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/687

0-1

1-2

2-3

3-4 4-5 Page **445** of **463** 6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21606	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/688
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21607	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/689
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx. adobe.com/se curity/produc	O-MIC- WIND- 030223/690

0-1

1-2

2-3

3-4 4-5 Page **446** of **463** 5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	ts/acrobat/ap sb23-01.html	
Out-of- bounds Write	18-Jan-2023	7.8	21608 Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21609	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/691
Stack- based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/692

0-1

1-2

 2-3
 3-4
 4-5

 Page
 447 of
 463

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21610		
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21611	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/693
Creation of Temporary File in Directory with Insecure Permission s	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/694

0-1

1-2

 2-3
 3-4
 4-5

 Page
 448 of
 463

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-		
Cleartext Transmissi on of Sensitive Informatio n	18-Jan-2023	5.9	21612 IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X- Force ID: 244109. CVE ID : CVE-2023- 22863	https://www. ibm.com/sup port/pages/n ode/6855837, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244109	O-MIC- WIND- 030223/695
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/696

0-1

1-2

2-3

3-4 4-5 Page **449** of **463** 5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2023- 21581		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023-	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/697
Use After Free	18-Jan-2023	5.5	21585 Adobe Dimension version 3.4.6 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx. adobe.com/se curity/produc ts/dimension /apsb23- 10.html	O-MIC- WIND- 030223/698

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21601		
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21603	https://helpx. adobe.com/se curity/produc ts/dimension /apsb23- 10.html	O-MIC- WIND- 030223/699
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21613	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/700

0-1

1-2

2-33-44-5Page 451 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Out-of- bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2023- 21614	https://helpx. adobe.com/se curity/produc ts/acrobat/ap sb23-01.html	O-MIC- WIND- 030223/701	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 244075. CVE ID : CVE-2023- 22594	https://www. ibm.com/sup port/pages/n ode/6855835, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244075	O-MIC- WIND- 030223/702	
Vendor: Omron						
Product: cp	11-el20dr-d_fir	mware				
Affected Ver	sion(s): *					

0-1

1-2

2-3

3-44-5Page 452 of 463

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
N/A	17-Jan-2023	9.8	Active debug code exists in OMRON CP1L- EL20DR-D all versions, which may lead to a command that is not specified in FINS protocol being executed without authentication. A remote unauthenticated attacker may read/write in arbitrary area of the device memory, which may lead to overwriting the firmware, causing a denial-of-service (DoS) condition, and/or arbitrary code execution. CVE ID : CVE-2023- 22357	N/A	O-OMR- CP1L- 030223/703	
Product: cx-	motion-mch_f	irmware				
Affected Vers	sion(s): * Up to	(excluding	g) 2.33			
Access of Uninitialize d Pointer	17-Jan-2023	7.8	CX-Motion-MCH v2.32 and earlier contains an access of uninitialized pointer vulnerability. Having a user to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution. CVE ID : CVE-2023-	N/A	0-0MR-CX- M- 030223/704	
			22366			
Vendor: Oracle						
Product: solaris Affected Version(s): 10						
N/A	18-Jan-2023	4	Vulnerability in the Oracle Solaris product	https://www. oracle.com/se	0-0RA-SOLA- 030223/705	
CVSS Scoring S	Scale 0-1	1-2 2	-3 3-4 4-5 5-6 Page 453 of 463	6-7 7-8	8-9 9-10	

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	4	Vulnerability in the Oracle Solaris product of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/ PR:H/UI:R/S:C/C:N/I:L /A:L).	https://www. oracle.com/se curity- alerts/cpujan 2023.html	O-ORA-SOLA- 030223/706

0-1

1-2

2-33-44-5Page 455 of 463

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21900		
Vendor: pix	ela				
Product: pix	x-rt100_firmwa	are			
Affected Ver	sion(s): 2.1.1_e	q101			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	8	OS command injection vulnerability in PIX- RT100 versions RT100_TEQ_2.1.1_EQ10 1 and RT100_TEQ_2.1.2_EQ10 1 allows a network- adjacent attacker who can access product settings to execute an arbitrary OS command. CVE ID : CVE-2023- 22304	https://www. pixela.co.jp/p roducts/netw ork/pix_rt100 /update.html	O-PIX-PIX 030223/707
N/A	17-Jan-2023	6.5	Hidden functionality vulnerability in PIX- RT100 versions RT100_TEQ_2.1.1_EQ10 1 and RT100_TEQ_2.1.2_EQ10 1 allows a network- adjacent attacker to access the product via undocumented Telnet or SSH services. CVE ID : CVE-2023- 22316	https://www. pixela.co.jp/p roducts/netw ork/pix_rt100 /update.html	O-PIX-PIX 030223/708
Affected Ver	sion(s): 2.1.2_e	, 101			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	17-Jan-2023	8	OS command injection vulnerability in PIX- RT100 versions RT100_TEQ_2.1.1_EQ10 1 and RT100_TEQ_2.1.2_EQ10 1 allows a network- adjacent attacker who can access product	https://www. pixela.co.jp/p roducts/netw ork/pix_rt100 /update.html	O-PIX-PIX 030223/709

0-1

1-2

2-33-44-5Page 456 of 463

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Command Injection')			settings to execute an arbitrary OS command.						
			CVE ID : CVE-2023- 22304						
N/A	17-Jan-2023	6.5	Hidden functionality vulnerability in PIX- RT100 versions RT100_TEQ_2.1.1_EQ10 1 and RT100_TEQ_2.1.2_EQ10 1 allows a network- adjacent attacker to access the product via undocumented Telnet or SSH services. CVE ID : CVE-2023- 22316	https://www. pixela.co.jp/p roducts/netw ork/pix_rt100 /update.html	O-PIX-PIX 030223/710				
Vendor: Red	Vendor: Redhat								
Product: op	enshift								
Affected Ver	sion(s): -								
Incorrect Permission Assignmen t for Critical Resource	18-Jan-2023	7.8	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.4 could allow a local user to perform unauthorized actions due to insufficient permission settings. IBM X-Force ID: 244073. CVE ID : CVE-2023- 22592	https://www. ibm.com/sup port/pages/n ode/6855839, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244073	O-RED- OPEN- 030223/711				
Cleartext Transmissi on of Sensitive Informatio n	18-Jan-2023	5.9	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain	https://www. ibm.com/sup port/pages/n ode/6855837, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244109	O-RED- OPEN- 030223/712				

0-1

1-2

2-3

3-4 4-5 Page **457** of **463** 8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information using man in the middle techniques. IBM X- Force ID: 244109.		
			CVE ID : CVE-2023- 22863		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 244075. CVE ID : CVE-2023- 22594	https://www. ibm.com/sup port/pages/n ode/6855835, https://excha nge.xforce.ib mcloud.com/v ulnerabilities/ 244075	O-RED- OPEN- 030223/713
Vendor: Son	nicwall				
	a1000_firmwa	ire			
Affected Vers	sion(s): 12.4.2				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-2023	7.5	Pre-authentication path traversal vulnerability in SMA1000 firmware version 12.4.2, which allows an unauthenticated attacker to access arbitrary files and directories stored outside the web root directory. CVE ID : CVE-2023-	https://psirt.g lobal.sonicwal l.com/vuln- detail/SNWLI D-2023-0001	O-SON- SMA1- 030223/714
			0126		

0-1

1-2

2-3

5-6

6-7 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ac	18_firmware	I		L	
Affected Ver	sion(s): 15.03.0	5.19			
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_000c231 8. CVE ID : CVE-2023- 24164	N/A	O-TEN-AC18- 030223/715
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/initIpAddrInfo CVE ID : CVE-2023- 24165	N/A	O-TEN-AC18- 030223/716
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/formWifiBasic Set. CVE ID : CVE-2023- 24166	N/A	O-TEN-AC18- 030223/717
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/add_white_no de. CVE ID : CVE-2023- 24167	N/A	O-TEN-AC18- 030223/718
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_0007343 c.	N/A	O-TEN-AC18- 030223/719

0-1

1-2

3-4 4-5 2-3 Page **459** of **463**

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2023- 24169			
Out-of- bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/fromSetWirel essRepeat.	N/A	O-TEN-AC18- 030223/720	
			CVE ID : CVE-2023- 24170			
Vendor: Tp	-link			I	<u> </u>	
Product: tl-	sg105pe_firmv	vare				
Affected Ver	sion(s): 1.0.0					
Improper Authentica tion	17-Jan-2023	9.8	TP-Link SG105PE firmware prior to 'TL- SG105PE(UN) 1.0_1.0.0 Build 20221208' contains an authentication bypass vulnerability. Under the certain conditions, an attacker may impersonate an administrator of the product. As a result, information may be obtained and/or the product's settings may be altered with the privilege of the administrator. CVE ID : CVE-2023- 22303	https://www. tp- link.com/jp/s upport/downl oad/tl- sg105pe/v1/ #Firmware, https://www. tp- link.com/en/ business- networking/e asy-smart- switch/tl- sg105pe/	O-TPTL-S- 030223/721	
Vendor: Tre	endnet			I	L	
Product: te	w-820ap_firmv	vare				
Affected Ver	sion(s): 1.01.b0	1				
Out-of- bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-	N/A	O-TRE-TEW 030223/722	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 460 of 463										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSystemCheck. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24095		
Out-of- bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the newpass parameter at /formPasswordSetup. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24096	N/A	O-TRE-TEW 030223/723
Out-of- bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware	N/A	0-TRE-TEW 030223/724

0-1

1-2

3-4 4-5 2-3 Page **461** of **463**

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formPasswordAuth. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023-		
Out-of- bounds Write	23-Jan-2023	8.8	24097 ** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSysLog. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. CVE ID : CVE-2023- 24098	N/A	O-TRE-TEW 030223/725
Out-of- bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW- 820AP v1.0R, firmware version 1.01.B01 was discovered to contain a	N/A	O-TRE-TEW 030223/726

0-1

1-2

2-33-44-5Page 462 of 463

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack overflow via the username parameter at		
			/formWizardPassword.		
			This vulnerability		
			allows attackers to		
			execute arbitrary code		
			via a crafted payload.		
			NOTE: This		
			vulnerability only affects products that		
			are no longer supported		
			by the maintainer.		
			CVE ID : CVE-2023-		
			24099		
Vendor: zep	hyrproject				
Product: zej	phyr				
Affected Ver	sion(s): * Up to	(including	g) 3.2.0		
			A malicious / defect bluetooth controller		
			can cause a Denial of		
Improper Initializatio n	19-Jan-2023		Service due to		
		6.5	unchecked input in	N/A	O-ZEP-ZEPH- 030223/727
			le_read_buffer_size_com plete.		
			•		
			CVE ID : CVE-2023- 0397		

0-1

1-2

2-3

6-7 7-8

5-6

9-10