تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 19 مايو إلى 25 مايو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
- عالي: النتيجة الأساسية لـCVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـCVSS 4.0-6.9
- منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 19th of May to 25th of May. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-29849	Veeam	Veeam Backup Enterprise Manager allows unauthenticated users to log in as any user to enterprise manager web interface.	2024-05-22	9.8	Critical
CVE-2024-5296	D-Link	D-Link D-View Use of Hard-coded Cryptographic Key Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the TokenUtils class. The issue results from a hard-coded cryptographic key. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-21991.	2024-05-23	9.8	Critical
CVE-2024-20360	Cisco	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface does not adequately validate user input. An attacker could exploit this vulnerability by authenticating to the application and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to obtain any data from the database, execute arbitrary commands on the underlying operating system, and elevate privileges to root. To exploit this vulnerability, an attacker would need at least Read Only user credentials.	2024-05-22	8.8	High
CVE-2024-29850	Veeam	Veeam Backup Enterprise Manager allows account takeover via NTLM relay.	2024-05-22	8.8	High
CVE-2024-5246	NETGEAR	NETGEAR ProSAFE Network Management System Tomcat Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the product installer. The issue results from the use of a vulnerable version of Apache Tomcat. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-22868.	2024-05-23	8.8	High
CVE-2024-5247	NETGEAR	NETGEAR ProSAFE Network Management System UpLoadServlet Unrestricted File Upload Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the UpLoadServlet class. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-22923.	2024-05-23	8.8	High

CVE-2024-5291	D-Link	D-Link DIR-2150 GetDeviceSettings Target Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21235.	2024-05-23	8.8	High
CVE-2024-5293	D-Link	D-Link DIR-2640 HTTP Referer Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2640-US routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within prog.cgi, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21853.	2024-05-23	8.8	High
CVE-2024-5295	D-Link	D-Link G416 flupl self Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 wireless routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21294.	2024-05-23	8.8	High
CVE-2024-5297	D-Link	D-Link D-View executeWmicCmd Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the executeWmicCmd method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21821.	2024-05-23	8.8	High
CVE-2024-5298	D-Link	D-Link D-View queryDeviceCustomMonitorResult Exposed Dangerous Method Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the queryDeviceCustomMonitorResult method. The issue results from an exposed dangerous method. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21842.	2024-05-23	8.8	High
CVE-2024-5299	D-Link	D-Link D-View execMonitorScript Exposed Dangerous Method Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the execMonitorScript method. The issue results from an exposed dangerous method. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21828.	2024-05-23	8.8	High
CVE-2023-49330	ManageEngine	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL Injection while getting aggregate report data.	2024-05-20	8.3	High
CVE-2023-49331	ManageEngine	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL injection in the aggregate reports search option.	2024-05-20	8.3	High
CVE-2023-49332	ManageEngine	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL injection while adding file shares.	2024-05-20	8.3	High
CVE-2023-49333	ManageEngine	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL injection in the dashboard graph feature.	2024-05-20	8.3	High
CVE-2023-49334	ManageEngine	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL Injection while exporting a full summary report.	2024-05-20	8.3	High

CVE-2023-49335	ManageEngine	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL injection while getting file server details.	2024-05-20	8.3	High
CVE-2024-27312	ManageEngine	Zoho ManageEngine PAM360 version 6601 is vulnerable to authorization vulnerability which allows a low-privileged user to perform admin actions. Note: This vulnerability affects only the PAM360 6600 version. No other versions are applicable to this vulnerability.	2024-05-20	8.1	High
CVE-2024-29000	SolarWinds	The SolarWinds Platform was determined to be affected by a reflected cross-site scripting vulnerability affecting the web console. A high-privileged user and user interaction is required to exploit this vulnerability.	2024-05-20	7.9	High
CVE-2023-52752	Linux	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix use-after-free bug in cifs_debug_data_proc_show() Skip SMB sessions that are being teared down (e.g. @ses->ses_status == SES_EXITING) in cifs_debug_data_proc_show() to avoid use-after-free in @ses. This fixes the following GPF when reading from /proc/fs/cifs/DebugData while mounting and umounting [816.251274] general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b6b81: 0000 [#1] PREEMPT SMP NOPTI ... [816.260138] Call Trace: [816.260329] <TASK> [816.260499] ? die_addr+0x36/0x90 [816.260762] ? exc_general_protection+0x1b3/0x410 [816.261126] ? asm_exc_general_protection+0x26/0x30 [816.261502] ? cifs_debug_tcon+0xbd/0x240 [cifs] [816.261878] ? cifs_debug_tcon+0xab/0x240 [cifs] [816.262249] cifs_debug_data_proc_show+0x516/0xdb0 [cifs] [816.262689] ? seq_read_iter+0x379/0x470 [816.262995] seq_read_iter+0x118/0x470 [816.263291] proc_reg_read_iter+0x53/0x90 [816.263596] ? srso_alias_return_thunk+0x5/0x7f [816.263945] vfs_read+0x201/0x350 [816.264211] ksys_read+0x75/0x100 [816.264472] do_syscall_64+0x3f/0x90 [816.264750] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [816.265135] RIP: 0033:0x7fd5e669d381	2024-05-21	7.8	High
CVE-2023-52760	Linux	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix slab-use-after-free in gfs2_qd_dealloc In gfs2_put_super(), whether withdrawn or not, the quota should be cleaned up by gfs2_quota_cleanup(). Otherwise, struct gfs2_sbd will be freed before gfs2_qd_dealloc (rcu callback) has run for all gfs2_quota_data objects, resulting in use-after-free. Also, gfs2_destroy_threads() and gfs2_quota_cleanup() is already called by gfs2_make_fs_ro(), so in gfs2_put_super(), after calling gfs2_make_fs_ro(), there is no need to call them again.	2024-05-21	7.8	High
CVE-2023-52769	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix htt mlo-offset event locking The ath12k active pdevs are protected by RCU but the htt mlo-offset event handling code calling ath12k_mac_get_ar_by_pdev_id() was not marked as a read-side critical section. Mark the code in question as an RCU read-side critical section to avoid any potential use-after-free issues. Compile tested only.	2024-05-21	7.8	High
CVE-2023-52772	Linux	In the Linux kernel, the following vulnerability has been resolved: af_unix: fix use-after-free in unix_stream_read_actor()	2024-05-21	7.8	High

		syzbot reported the following crash [1] After releasing unix socket lock, u->oob_skb can be changed by another thread. We must temporarily increase skb refcount to make sure this other thread will not free the skb under us. [1] BUG: KASAN: slab-use-after-free in unix_stream_read_actor+0xa7/0xc0 net/unix/af_unix.c:2866 Read of size 4 at addr ffff88801f3b9cc4 by task syz- executor107/5297 CPU: 1 PID: 5297 Comm: syz-executor107 Not tainted 6.6.0- syzkaller-15910-gb8e3a87a627b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/09/2023 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd9/0x1b0 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:364 [inline] print_report+0xc4/0x620 mm/kasan/report.c:475 kasan_report+0xda/0x110 mm/kasan/report.c:588 unix_stream_read_actor+0xa7/0xc0 net/unix/af_unix.c:2866 unix_stream_recv_urg net/unix/af_unix.c:2587 [inline] unix_stream_read_generic+0x19a5/0x2480 net/unix/af_unix.c:2666 unix_stream_recvmsg+0x189/0x1b0 net/unix/af_unix.c:2903 sock_recvmsg_nosec net/socket.c:1044 [inline] sock_recvmsg+0xe2/0x170 net/socket.c:1066 ____sys_recvmsg+0x21f/0x5c0 net/socket.c:2803 ___sys_recvmsg+0x115/0x1a0 net/socket.c:2845 __sys_recvmsg+0x114/0x1e0 net/socket.c:2875 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x3f/0x110 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x63/0x6b RIP: 0033:0x7fc67492c559 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fc6748ab228 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 000000000000001c RCX: 00007fc67492c559 RDX: 0000000040010083 RSI: 0000000020000140 RDI: 0000000000000004 RBP: 00007fc6749b6348 R08: 00007fc6748ab6c0 R09: 00007fc6748ab6c0 R10: 0000000000000000 R11: 0000000000000246 R12: 00007fc6749b6340 R13: 00007fc6749b634c R14: 00007ffe9fac52a0 R15: 00007ffe9fac5388 </TASK> Allocated by task 5295: kasan_save_stack+0x33/0x50 mm/kasan/common.c:45 kasan_set_track+0x25/0x30 mm/kasan/common.c:52 __kasan_slab_alloc+0x81/0x90 mm/kasan/common.c:328 kasan_slab_alloc include/linux/kasan.h:188 [inline] slab_post_alloc_hook mm/slab.h:763 [inline] slab_alloc_node mm/slub.c:3478 [inline] kmem_cache_alloc_node+0x180/0x3c0 mm/slub.c:3523 __alloc_skb+0x287/0x330 net/core/skbuff.c:641 alloc_skb include/linux/skbuff.h:1286 [inline] alloc_skb_with_frags+0xe4/0x710 net/core/skbuff.c:6331 sock_alloc_send_pskb+0x7e4/0x970 net/core/sock.c:2780 sock_alloc_send_skb include/net/sock.h:1884 [inline] queue_oob net/unix/af_unix.c:2147 [inline] unix_stream_sendmsg+0xb5f/0x10a0 net/unix/af_unix.c:2301 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0xd5/0x180 net/socket.c:745 ____sys_sendmsg+0x6ac/0x940 net/socket.c:2584 ___sys_sendmsg+0x135/0x1d0 net/socket.c:2638 __sys_sendmsg+0x117/0x1e0 net/socket.c:2667 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x3f/0x110 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x63/0x6b Freed by task 5295:			

		kasan_save_stack+0x33/0x50 mm/kasan/common.c:45 kasan_set_track+0x25/0x30 mm/kasan/common.c:52 kasan_save_free_info+0x2b/0x40 mm/kasan/generic.c:522 ____kasan_slab_free mm/kasan/common.c:236 [inline] ____kasan_slab_free+0x15b/0x1b0 mm/kasan/common.c:200 kasan_slab_free include/linux/kasan.h:164 [inline] slab_free_hook mm/slub.c:1800 [inline] slab_free_freelist_hook+0x114/0x1e0 mm/slub.c:1826 slab_free mm/slub.c:3809 [inline] kmem_cache_free+0xf8/0x340 mm/slub.c:3831 kfree_skbmem+0xef/0x1b0 net/core/skbuff.c:1015 __kfree_skb net/core/skbuff.c:1073 [inline] consume_skb net/core/skbuff.c:1288 [inline] consume_skb+0xdf/0x170 net/core/skbuff.c:1282 queue_oob net/unix/af_unix.c:2178 [inline] u ---truncated---			
CVE-2024-29853	Veeam	An authentication bypass vulnerability in Veeam Agent for Microsoft Windows allows for local privilege escalation.	2024-05-22	7.8	High
CVE-2024-30279	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 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.	2024-05-23	7.8	High
CVE-2024-30280	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-23	7.8	High
CVE-2024-5245	NETGEAR	NETGEAR ProSAFE Network Management System Default Credentials Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the product installer. The issue results from the use of default MySQL credentials. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-22755.	2024-05-23	7.8	High
CVE-2024-5227	TP-Link	TP-Link Omada ER605 PPTP VPN username Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are only vulnerable if configured to use a PPTP VPN with LDAP authentication. The specific flaw exists within the handling of the username parameter provided to the /usr/bin/pppd endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22446.	2024-05-23	7.5	High
CVE-2024-5228	TP-Link	TP-Link Omada ER605 Comexe DDNS Response Handling Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the handling of DNS responses. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22383.	2024-05-23	7.5	High
CVE-2024-5242	TP-Link	TP-Link Omada ER605 Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the handling of DDNS error codes. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based	2024-05-23	7.5	High

		buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22522.			
CVE-2024-5243	TP-Link	TP-Link Omada ER605 Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the handling of DNS names. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22523.	2024-05-23	7.5	High
CVE-2024-27264	IBM	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 could allow a local user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 284563.	2024-05-22	7.4	High
CVE-2024-5292	D-Link	D-Link Network Assistant Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of D-Link Network Assistant. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the DNACore service. The service loads a file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-21426.	2024-05-23	7.3	High
CVE-2024-29851	Veeam	Veeam Backup Enterprise Manager allows high-privileged users to steal NTLM hash of Enterprise manager service account.	2024-05-22	7.2	High
CVE-2023-52827	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix possible out-of-bound read in ath12k_htt_pull_ppdu_stats() len is extracted from HTT message and could be an unexpected value in case errors happen, so add validation before using to avoid possible out-of-bound read in the following message iteration and parsing. The same issue also applies to ppdu_info->ppdu_stats.common.num_users, so validate it before using too. These are found during code review. Compile test only.	2024-05-21	7.1	High
CVE-2024-30056	Microsoft	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-05-25	7.1	High
CVE-2023-46806	Ivanti	An SQL Injection vulnerability in a web component of EPMM versions before 12.1.0.0 allows an authenticated user with appropriate privilege to access or modify data in the underlying database.	2024-05-22	6.7	Medium
CVE-2023-46807	Ivanti	An SQL Injection vulnerability in web component of EPMM before 12.1.0.0 allows an authenticated user with appropriate privilege to access or modify data in the underlying database.	2024-05-22	6.7	Medium
CVE-2024-22026	Ivanti	A local privilege escalation vulnerability in EPMM before 12.1.0.0 allows an authenticated local user to bypass shell restriction and execute arbitrary commands on the appliance.	2024-05-22	6.7	Medium
CVE-2023-37929	Zyxel	The buffer overflow vulnerability in the CGI program of the VMG3625-T50B firmware version V5.50(ABPM.8)C0 could allow an authenticated remote attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	2024-05-21	6.5	Medium
CVE-2024-31904	IBM	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.25 and 12.0.1.0 through 12.0.12.0 integration nodes could allow an authenticated user to cause a denial of service due to an uncaught exception. IBM X-Force ID: 289647.	2024-05-22	6.5	Medium
CVE-2024-20261	Cisco	A vulnerability in the file policy feature that is used to inspect encrypted archive files of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured file policy to block an encrypted archive file. This vulnerability exists because of a logic error when a specific class of encrypted archive files is inspected. An attacker could exploit this vulnerability by sending a crafted, encrypted archive file through the affected device. A successful exploit could allow the attacker to send an encrypted archive file, which could contain	2024-05-22	5.8	Medium

		malware and should have been blocked and dropped at the Cisco FTD device.			
CVE-2024-20293	Cisco	A vulnerability in the activation of an access control list (ACL) on Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the protection that is offered by a configured ACL on an affected device. This vulnerability is due to a logic error that occurs when an ACL changes from inactive to active in the running configuration of an affected device. An attacker could exploit this vulnerability by sending traffic through the affected device that should be denied by the configured ACL. The reverse condition is also true—traffic that should be permitted could be denied by the configured ACL. A successful exploit could allow the attacker to bypass configured ACL protections on the affected device, allowing the attacker to access trusted networks that the device might be protecting. Note: This vulnerability applies to both IPv4 and IPv6 traffic as well as dual-stack ACL configurations in which both IPv4 and IPv6 ACLs are configured on an interface.	2024-05-22	5.8	Medium
CVE-2024-20361	Cisco	A vulnerability in the Object Groups for Access Control Lists (ACLs) feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass configured access controls on managed devices that are running Cisco Firepower Threat Defense (FTD) Software. This vulnerability is due to the incorrect deployment of the Object Groups for ACLs feature from Cisco FMC Software to managed FTD devices in high-availability setups. After an affected device is rebooted following Object Groups for ACLs deployment, an attacker can exploit this vulnerability by sending traffic through the affected device. A successful exploit could allow the attacker to bypass configured access controls and successfully send traffic to devices that are expected to be protected by the affected device.	2024-05-22	5.8	Medium
CVE-2024-20363	Cisco	Multiple Cisco products are affected by a vulnerability in the Snort Intrusion Prevention System (IPS) rule engine that could allow an unauthenticated, remote attacker to bypass the configured rules on an affected system. This vulnerability is due to incorrect HTTP packet handling. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured IPS rules and allow uninspected traffic onto the network.	2024-05-22	5.8	Medium
CVE-2024-35972	Linux	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Fix possible memory leak in bnxt_rdma_aux_device_init() If ulp = kzalloc() fails, the allocated edev will leak because it is not properly assigned and the cleanup path will not be able to free it. Fix it by assigning it properly immediately after allocation.	2024-05-20	5.5	Medium
CVE-2024-35978	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix memory leak in hci_req_sync_complete() In 'hci_req_sync_complete()', always free the previous sync request state before assigning reference to a new one.	2024-05-20	5.5	Medium
CVE-2024-35982	Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: Avoid infinite loop trying to resize local TT If the MTU of one of an attached interface becomes too small to transmit the local translation table then it must be resized to fit inside all fragments (when enabled) or a single packet. But if the MTU becomes too low to transmit even the header + the VLAN specific part then the resizing of the local TT will never succeed. This can for example happen when the usable space is 110 bytes and 11 VLANs are on top of batman-adv. In this case, at least 116 byte would be needed. There will just be an endless spam of batman_adv: batadv0: Forced to purge local tt entries to fit new maximum fragment MTU (110) in the log but the function will never finish. Problem here is that the timeout will be halved all the time and will then stagnate at 0 and therefore never be able to reduce the table even more.	2024-05-20	5.5	Medium

		There are other scenarios possible with a similar result. The number of BATADV_TT_CLIENT_NOPURGE entries in the local TT can for example be too high to fit inside a packet. Such a scenario can therefore happen also with only a single VLAN + 7 non-purgable addresses - requiring at least 120 bytes. While this should be handled proactively when: * interface with too low MTU is added * VLAN is added * non-purgeable local mac is added * MTU of an attached interface is reduced * fragmentation setting gets disabled (which most likely requires dropping attached interfaces) not all of these scenarios can be prevented because batman-adv is only consuming events without the the possibility to prevent these actions (non-purgable MAC address added, MTU of an attached interface is reduced). It is therefore necessary to also make sure that the code is able to handle also the situations when there were already incompatible system configuration are present.			
CVE-2024-35984	Linux	In the Linux kernel, the following vulnerability has been resolved: i2c: smbus: fix NULL function pointer dereference Baruch reported an OOPS when using the designware controller as target only. Target-only modes break the assumption of one transfer function always being available. Fix this by always checking the pointer in __i2c_transfer. [wsa: dropped the simplification in core-smbus to avoid theoretical regressions]	2024-05-20	5.5	Medium
CVE-2024-35990	Linux	In the Linux kernel, the following vulnerability has been resolved: dma: xilinx_dpdma: Fix locking There are several places where either chan->lock or chan->vchan.lock was not held. Add appropriate locking. This fixes lockdep warnings like [31.077578] ------------[cut here]------------ [31.077831] WARNING: CPU: 2 PID: 40 at drivers/dma/xilinx/xilinx_dpdma.c:834 xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.077953] Modules linked in: [31.078019] CPU: 2 PID: 40 Comm: kworker/u12:1 Not tainted 6.6.20+ #98 [31.078102] Hardware name: xlnx,zynqmp (DT) [31.078169] Workqueue: events_unbound deferred_probe_work_func [31.078272] pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [31.078377] pc : xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.078473] lr : xilinx_dpdma_chan_queue_transfer+0x270/0x5e0 [31.078550] sp : ffffffc083bb2e10 [31.078590] x29: ffffffc083bb2e10 x28: 0000000000000000 x27: ffffff880165a168 [31.078754] x26: ffffff880164e920 x25: ffffff880164eab8 x24: ffffff880164d480 [31.078920] x23: ffffff880165a148 x22: ffffff880164e988 x21: 0000000000000000 [31.079132] x20: ffffffc082aa3000 x19: ffffff880164e880 x18: 0000000000000000 [31.079295] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [31.079453] x14: 0000000000000000 x13: ffffff8802263dc0 x12:	2024-05-20	5.5	Medium

		0000000000000001 [31.079613] x11: 0001ffc083bb2e34 x10: 0001ff880164e98f x9 : 0001ffc082aa3def [31.079824] x8 : 0001ffc082aa3dec x7 : 0000000000000000 x6 : 0000000000000516 [31.079982] x5 : ffffffc7f8d43000 x4 : ffffff88003c9c40 x3 : ffffffffffffffff [31.080147] x2 : ffffffc7f8d43000 x1 : 00000000000000c0 x0 : 0000000000000000 [31.080307] Call trace: [31.080340] xilinx_dpdma_chan_queue_transfer+0x274/0x5e0 [31.080518] xilinx_dpdma_issue_pending+0x11c/0x120 [31.080595] zynqmp_disp_layer_update+0x180/0x3ac [31.080712] zynqmp_dpsub_plane_atomic_update+0x11c/0x21c [31.080825] drm_atomic_helper_commit_planes+0x20c/0x684 [31.080951] drm_atomic_helper_commit_tail+0x5c/0xb0 [31.081139] commit_tail+0x234/0x294 [31.081246] drm_atomic_helper_commit+0x1f8/0x210 [31.081363] drm_atomic_commit+0x100/0x140 [31.081477] drm_client_modeset_commit_atomic+0x318/0x384 [31.081634] drm_client_modeset_commit_locked+0x8c/0x24c [31.081725] drm_client_modeset_commit+0x34/0x5c [31.081812] __drm_fb_helper_restore_fbdev_mode_unlocked+0x104/0x168 [31.081899] drm_fb_helper_set_par+0x50/0x70 [31.081971] fbcon_init+0x538/0xc48 [31.082047] visual_init+0x16c/0x23c [31.082207] do_bind_con_driver.isra.0+0x2d0/0x634 [31.082320] do_take_over_console+0x24c/0x33c [31.082429] do_fbcon_takeover+0xbc/0x1b0 [31.082503] fbcon_fb_registered+0x2d0/0x34c [31.082663] register_framebuffer+0x27c/0x38c [31.082767] __drm_fb_helper_initial_config_and_unlock+0x5c0/0x91c [31.082939] drm_fb_helper_initial_config+0x50/0x74 [31.083012] drm_fbdev_dma_client_hotplug+0xb8/0x108 [31.083115] drm_client_register+0xa0/0xf4 [31.083195] drm_fbdev_dma_setup+0xb0/0x1cc [31.083293] zynqmp_dpsub_drm_init+0x45c/0x4e0 [31.083431] zynqmp_dpsub_probe+0x444/0x5e0 [31.083616] platform_probe+0x8c/0x13c [31.083713] really_probe+0x258/0x59c [31.083793] __driver_probe_device+0xc4/0x224 [31.083878] driver_probe_device+0x70/0x1c0 [31.083961] __device_attach_driver+0x108/0x1e0 [31.084052] bus_for_each_drv+0x9c/0x100 [31.084125] __device_attach+0x100/0x298 [31.084207] device_initial_probe+0x14/0x20 [31.084292] bus_probe_device+0xd8/0xdc [31.084368] deferred_probe_work_func+0x11c/0x180 [31.084451] process_one_work+0x3ac/0x988 [31.084643] worker_thread+0x398/0x694 [31.084752] kthread+0x1bc/0x1c0 [31.084848] ret_from_fork+0x10/0x20 [31.084932] irq event stamp: 64549 [31.084970] hardirqs last enabled at (64548): [<ffffffc081adf35c>] _raw_spin_unlock_irqrestore+0x80/0x90 [31.085157] ---truncated---			
CVE-2024-35992	Linux	In the Linux kernel, the following vulnerability has been resolved: phy: marvell: a3700-comphy: Fix out of bounds read There is an out of bounds read access of 'gbe_phy_init_fix[fix_idx].addr' every iteration after 'fix_idx' reaches 'ARRAY_SIZE(gbe_phy_init_fix)'. Make sure 'gbe_phy_init[addr]' is used when all elements of 'gbe_phy_init_fix' array are handled. Found by Linux Verification Center (linuxtesting.org) with SVACE.	2024-05-20	5.5	Medium
CVE-2024-35997	Linux	In the Linux kernel, the following vulnerability has been resolved: HID: i2c-hid: remove I2C_HID_READ_PENDING flag to prevent lock-up The flag I2C_HID_READ_PENDING is used to serialize I2C operations.	2024-05-20	5.5	Medium

		However, this is not necessary, because I2C core already has its own locking for that. More importantly, this flag can cause a lock-up: if the flag is set in i2c_hid_xfer() and an interrupt happens, the interrupt handler (i2c_hid_irq) will check this flag and return immediately without doing anything, then the interrupt handler will be invoked again in an infinite loop. Since interrupt handler is an RT task, it takes over the CPU and the flag-clearing task never gets scheduled, thus we have a lock-up. Delete this unnecessary flag.			
CVE-2024-36008	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv4: check for NULL idev in ip_route_use_hint() syzbot was able to trigger a NULL deref in fib_validate_source() in an old tree [1]. It appears the bug exists in latest trees. All calls to __in_dev_get_rcu() must be checked for a NULL result. [1] general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] SMP KASAN KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] CPU: 2 PID: 3257 Comm: syz-executor.3 Not tainted 5.10.0-syzkaller #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 RIP: 0010:fib_validate_source+0xbf/0x15a0 net/ipv4/fib_frontend.c:425 Code: 18 f2 f2 f2 f2 42 c7 44 20 23 f3 f3 f3 f3 48 89 44 24 78 42 c6 44 20 27 f3 e8 5d 88 48 fc 4c 89 e8 48 c1 e8 03 48 89 44 24 18 <42> 80 3c 20 00 74 08 4c 89 ef e8 d2 15 98 fc 48 89 5c 24 10 41 bf RSP: 0018:ffffc900015fee40 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff88800f7a4000 RCX: ffff88800f4f90c0 RDX: 0000000000000000 RSI: 0000000004001eac RDI: ffff8880160c64c0 RBP: ffffc900015ff060 R08: 0000000000000000 R09: ffff88800f7a4000 R10: 0000000000000002 R11: ffff88800f4f90c0 R12: dffffc0000000000 R13: 0000000000000000 R14: 0000000000000000 R15: ffff88800f7a4000 FS: 00007f938acfe6c0(0000) GS:ffff888058c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f938acddd58 CR3: 000000001248e000 CR4: 0000000000352ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: ip_route_use_hint+0x410/0x9b0 net/ipv4/route.c:2231 ip_rcv_finish_core+0x2c4/0x1a30 net/ipv4/ip_input.c:327 ip_list_rcv_finish net/ipv4/ip_input.c:612 [inline] ip_sublist_rcv+0x3ed/0xe50 net/ipv4/ip_input.c:638 ip_list_rcv+0x422/0x470 net/ipv4/ip_input.c:673 __netif_receive_skb_list_ptype net/core/dev.c:5572 [inline] __netif_receive_skb_list_core+0x6b1/0x890 net/core/dev.c:5620 __netif_receive_skb_list net/core/dev.c:5672 [inline] netif_receive_skb_list_internal+0x9f9/0xdc0 net/core/dev.c:5764 netif_receive_skb_list+0x55/0x3e0 net/core/dev.c:5816 xdp_recv_frames net/bpf/test_run.c:257 [inline] xdp_test_run_batch net/bpf/test_run.c:335 [inline] bpf_test_run_xdp_live+0x1818/0x1d00 net/bpf/test_run.c:363 bpf_prog_test_run_xdp+0x81f/0x1170 net/bpf/test_run.c:1376 bpf_prog_test_run+0x349/0x3c0 kernel/bpf/syscall.c:3736 __sys_bpf+0x45c/0x710 kernel/bpf/syscall.c:5115 __do_sys_bpf kernel/bpf/syscall.c:5201 [inline] __se_sys_bpf kernel/bpf/syscall.c:5199 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5199	2024-05-20	5.5	Medium

CVE-2024-0816	Zyxel	The buffer overflow vulnerability in the DX3300-T1 firmware version V5.50(ABVY.4)C0 could allow an authenticated local attacker to cause denial of service (DoS) conditions by executing the CLI command with crafted strings on an affected device.	2024-05-21	5.5	Medium
CVE-2023-52753	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid NULL dereference of timing generator [Why & How] Check whether assigned timing generator is NULL or not before accessing its funcs to prevent NULL dereference.	2024-05-21	5.5	Medium
CVE-2023-52773	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix a NULL pointer dereference in amdgpu_dm_i2c_xfer() When ddc_service_construct() is called, it explicitly checks both the link type and whether there is something on the link which will dictate whether the pin is marked as hw_supported. If the pin isn't set or the link is not set (such as from unloading/reloading amdgpu in an IGT test) then fail the amdgpu_dm_i2c_xfer() call.	2024-05-21	5.5	Medium
CVE-2023-52783	Linux	In the Linux kernel, the following vulnerability has been resolved: net: wangxun: fix kernel panic due to null pointer When the device uses a custom subsystem vendor ID, the function wx_sw_init() returns before the memory of 'wx->mac_table' is allocated. The null pointer will causes the kernel panic.	2024-05-21	5.5	Medium
CVE-2023-52802	Linux	In the Linux kernel, the following vulnerability has been resolved: iio: adc: stm32-adc: harden against NULL pointer deref in stm32_adc_probe() of_match_device() may fail and returns a NULL pointer. In practice there is no known reasonable way to trigger this, but in case one is added in future, harden the code by adding the check	2024-05-21	5.5	Medium
CVE-2023-52806	Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: Fix possible null-ptr-deref when assigning a stream While AudioDSP drivers assign streams exclusively of HOST or LINK type, nothing blocks a user to attempt to assign a COUPLED stream. As supplied substream instance may be a stub, what is the case when code-loading, such scenario ends with null-ptr-deref.	2024-05-21	5.5	Medium
CVE-2023-52809	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: libfc: Fix potential NULL pointer dereference in fc_lport_ptp_setup() fc_lport_ptp_setup() did not check the return value of fc_rport_create() which can return NULL and would cause a NULL pointer dereference. Address this issue by checking return value of fc_rport_create() and log error message on fc_rport_create() failed.	2024-05-21	5.5	Medium
CVE-2023-52814	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix potential null pointer derefernce The amdgpu_ras_get_context may return NULL if device not support ras feature, so add check before using.	2024-05-21	5.5	Medium
CVE-2023-52815	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vkms: fix a possible null pointer dereference In amdgpu_vkms_conn_get_modes(), the return value of drm_cvt_mode() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_cvt_mode(). Add a check to avoid null pointer dereference.	2024-05-21	5.5	Medium
CVE-2023-52817	Linux	In the Linux kernel, the following vulnerability has been resolved:	2024-05-21	5.5	Medium

		drm/amdgpu: Fix a null pointer access when the smc_rreg pointer is NULL In certain types of chips, such as VEGA20, reading the amdgpu_regs_smc file could result in an abnormal null pointer access when the smc_rreg pointer is NULL. Below are the steps to reproduce this issue and the corresponding exception log: 1. Navigate to the directory: /sys/kernel/debug/dri/0 2. Execute command: cat amdgpu_regs_smc 3. Exception Log:: [4005007.702554] BUG: kernel NULL pointer dereference, address: 0000000000000000 [4005007.702562] #PF: supervisor instruction fetch in kernel mode [4005007.702567] #PF: error_code(0x0010) - not-present page [4005007.702570] PGD 0 P4D 0 [4005007.702576] Oops: 0010 [#1] SMP NOPTI [4005007.702581] CPU: 4 PID: 62563 Comm: cat Tainted: G OE 5.15.0-43-generic #46-Ubunt u [4005007.702590] RIP: 0010:0x0 [4005007.702598] Code: Unable to access opcode bytes at RIP 0xffffffffffffffd6. [4005007.702600] RSP: 0018:ffffa82b46d27da0 EFLAGS: 00010206 [4005007.702605] RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffffa82b46d27e68 [4005007.702609] RDX: 0000000000000001 RSI: 0000000000000000 RDI: ffff9940656e0000 [4005007.702612] RBP: ffffa82b46d27dd8 R08: 0000000000000000 R09: ffff994060c07980 [4005007.702615] R10: 0000000000020000 R11: 0000000000000000 R12: 00007f5e06753000 [4005007.702618] R13: ffff9940656e0000 R14: ffffa82b46d27e68 R15: 00007f5e06753000 [4005007.702622] FS: 00007f5e0755b740(0000) GS:ffff99479d300000(0000) knlGS:0000000000000000 [4005007.702626] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [4005007.702629] CR2: ffffffffffffffd6 CR3: 00000003253fc000 CR4: 00000000003506e0 [4005007.702633] Call Trace: [4005007.702636] <TASK> [4005007.702640] amdgpu_debugfs_regs_smc_read+0xb0/0x120 [amdgpu] [4005007.703002] full_proxy_read+0x5c/0x80 [4005007.703011] vfs_read+0x9f/0x1a0 [4005007.703019] ksys_read+0x67/0xe0 [4005007.703023] __x64_sys_read+0x19/0x20 [4005007.703028] do_syscall_64+0x5c/0xc0 [4005007.703034] ? do_user_addr_fault+0x1e3/0x670 [4005007.703040] ? exit_to_user_mode_prepare+0x37/0xb0 [4005007.703047] ? irqentry_exit_to_user_mode+0x9/0x20 [4005007.703052] ? irqentry_exit+0x19/0x30 [4005007.703057] ? exc_page_fault+0x89/0x160 [4005007.703062] ? asm_exc_page_fault+0x8/0x30 [4005007.703068] entry_SYSCALL_64_after_hwframe+0x44/0xae [4005007.703075] RIP: 0033:0x7f5e07672992 [4005007.703079] Code: c0 e9 b2 fe ff ff 50 48 8d 3d fa b2 0c 00 e8 c5 1d 02 00 0f 1f 44 00 00 f3 0f 1e fa 64 8b 04 25 18 00 00 00 85 c0 75 10 0f 05 <48> 3d 00 f0 ff ff 77 56 c3 0f 1f 44 00 00 48 83 e c 28 48 89 54 24 [4005007.703083] RSP: 002b:00007ffe03097898 EFLAGS: 00000246 ORIG_RAX: 0000000000000000 [4005007.703088] RAX: ffffffffffffffda RBX: 0000000000020000 RCX: 00007f5e07672992 [4005007.703091] RDX: 0000000000020000 RSI: 00007f5e06753000 RDI: 0000000000000003 [4005007.703094] RBP: 00007f5e06753000 R08: 00007f5e06752010 R09: 00007f5e06752010 [4005007.703096] R10: 0000000000000022 R11: 0000000000000246 R12: 0000000000022000 [4005007.703099] R13: 0000000000000003 R14: 0000000000020000 R15: 0000000000020000 [4005007.703105] </TASK> [4005007.703107] Modules linked in: nf_tables libcrc32c nfnetlink algif_hash af_alg binfmt_misc nls_ iso8859_1 ipmi_ssif ast intel_rapl_msr intel_rapl_common drm_vram_helper drm_ttm_helper amd64_edac t tm edac_mce_amd kvm_amd ccp mac_hid k10temp kvm acpi_ipmi ipmi_si rapl sch_fq_codel ipmi_devintf ipm i_msghandler msr parport_pc ppdev lp parport mtd pstore_blk efi_pstore ramoops pstore_zone			

		reed_solo mon ip_tables x_tables autofs4 ib_uverbs ib_core amdgpu(OE) amddrm_ttm_helper(OE) amdttm(OE) iommu_v 2 amd_sched(OE) amdkcl(OE) drm_kms_helper syscopyarea sysfillrect sysimgblt fb_sys_fops cec rc_core drm igb ahci xhci_pci libahci i2c_piix4 i2c_algo_bit xhci_pci_renesas dca [4005007.703184] CR2: 0000000000000000 [4005007.703188] ---[en ---truncated---			
CVE-2023-52821	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/panel: fix a possible null pointer dereference In versatile_panel_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	2024-05-21	5.5	Medium
CVE-2023-47710	IBM	IBM Security Guardium 11.4, 11.5, and 12.0 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: 271525.	2024-05-24	5.4	Medium
CVE-2020-35165	Dell	Dell BSAFE Crypto-C Micro Edition, versions before 4.1.5, and Dell BSAFE Micro Edition Suite, versions before 4.6, contain an Observable Timing Discrepancy Vulnerability.	2024-05-22	5.1	Medium
CVE-2024-20355	Cisco	A vulnerability in the implementation of SAML 2.0 single sign-on (SSO) for remote access VPN services in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to successfully establish a VPN session on an affected device. This vulnerability is due to improper separation of authorization domains when using SAML authentication. An attacker could exploit this vulnerability by using valid credentials to successfully authenticate using their designated connection profile (tunnel group), intercepting the SAML SSO token that is sent back from the Cisco ASA device, and then submitting the same SAML SSO token to a different tunnel group for authentication. A successful exploit could allow the attacker to establish a remote access VPN session using a connection profile that they are not authorized to use and connect to secured networks behind the affected device that they are not authorized to access. For successful exploitation, the attacker must have valid remote access VPN user credentials.	2024-05-22	5	Medium
CVE-2024-5244	TP-Link	TP-Link Omada ER605 Reliance on Security Through Obscurity Vulnerability. This vulnerability allows network-adjacent attackers to access or spoof DDNS messages on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. However, devices are vulnerable only if configured to use the Comexe DDNS service. The specific flaw exists within the cmxddnsd executable. The issue results from reliance on obscurity to secure network data. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-22439.	2024-05-23	5	Medium
CVE-2024-21791	ManageEngine	Zoho ManageEngine ADAudit Plus versions below 7271 allows SQL Injection in lockout history option. Note: Non-admin users cannot exploit this vulnerability.	2024-05-22	4.7	Medium
CVE-2024-31893	IBM	IBM App Connect Enterprise 12.0.1.0 through 12.0.12.1 could allow an authenticated user to obtain sensitive calendar information using an expired access token. IBM X-Force ID: 288174.	2024-05-22	4.3	Medium
CVE-2024-31894	IBM	IBM App Connect Enterprise 12.0.1.0 through 12.0.12.1 could allow an authenticated user to obtain sensitive user information using an expired access token. IBM X-Force ID: 288175.	2024-05-22	4.3	Medium
CVE-2024-31895	IBM	IBM App Connect Enterprise 12.0.1.0 through 12.0.12.1 could allow an authenticated user to obtain sensitive user information using an expired access token. IBM X-Force ID: 288176.	2024-05-22	4.3	Medium
CVE-2024-5294	D-Link	D-Link DIR-3040 prog.cgi websSecurityHandler Memory Leak Denial-of-Service Vulnerability. This vulnerability allows network-adjacent attackers to create a denial-of-service condition on affected installations of D-Link DIR-3040 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the prog.cgi program, which handles HNAP requests made to the lighttpd webserver listening on ports 80 and 443. The issue results from the lack of proper memory management when processing HTTP cookie values. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. . Was ZDI-CAN-21668.	2024-05-23	4.3	Medium

CVE-2024-29852	Veeam	Veeam Backup Enterprise Manager allows high-privileged users to read backup session logs.	2024-05-22	2.7	Low

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.