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 ٢٣ يونيو إلى ٢٩ يونيو. 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 23rd of June to 29th of June. 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-2024-39462	Linux	In the Linux kernel, the following vulnerability has been resolved: clk: bcm: dvp: Assign ->num before accessing ->hws Commit f316cdff8d67 ("clk: Annotate struct clk_hw_onecell_data with __counted_by") annotated the hws member of 'struct clk_hw_onecell_data' with __counted_by, which informs the bounds sanitizer about the number of elements in hws, so that it can warn when hws is accessed out of bounds. As noted in that change, the __counted_by member must be initialized with the number of elements before the first array access happens, otherwise there will be a warning from each access prior to the initialization because the number of elements is zero. This occurs in clk_dvp_probe() due to ->num being assigned after ->hws has been accessed: UBSAN: array-index-out-of-bounds in drivers/clk/bcm/clk-bcm2711-dvp.c:59:2 index 0 is out of range for type 'struct clk_hw *[] __counted_by(num)' (aka 'struct clk_hw *[]') Move the ->num initialization to before the first access of ->hws, which clears up the warning.	2024-06-25	9.8	Critical
CVE-2024-39349	Synology	A vulnerability regarding buffer copy without checking size of input ('Classic Buffer Overflow') is found in the libjansson component and it does not affect the upstream library. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	9.8	Critical
CVE-2024-5535	OpenSSL	Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from	2024-06-27	9.1	Critical

		memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a "no overlap" response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications			

		are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available.			
CVE-2021-4440	Linux	In the Linux kernel, the following vulnerability has been resolved: x86/xen: Drop USERGS_SYSRET64 paravirt call commit afd30525a659ac0ae0904f0cb4a2ca75522c3123 upstream. USERGS_SYSRET64 is used to return from a syscall via SYSRET, but a Xen PV guest will nevertheless use the IRET hypercall, as there is no sysret PV hypercall defined. So instead of testing all the prerequisites for doing a sysret and then mangling the stack for Xen PV again for doing an iret just use the iret exit from the beginning. This can easily be done via an ALTERNATIVE like it is done for the sysenter compat case already. It should be noted that this drops the optimization in Xen for not restoring a few registers when returning to user mode, but it seems as if the saved instructions in the kernel more than compensate for this drop (a kernel build in a Xen PV guest was slightly faster with this patch applied). While at it remove the stale sysret32 remnants. [pawan: Brad Spengler and Salvatore Bonaccorso <carnil@debian.org> reported a problem with the 5.10 backport commit edc702b4a820 ("x86/entry_64: Add VERW just before userspace transition"). When CONFIG_PARAVIRT_XXL=y, CLEAR_CPU_BUFFERS is not executed in syscall_return_via_sysret path as USERGS_SYSRET64 is runtime patched to: .cpu_usergs_sysret64 = { 0x0f, 0x01, 0xf8, 0x48, 0x0f, 0x07 }, // swapgs; sysretq which is missing CLEAR_CPU_BUFFERS. It turns out dropping USERGS_SYSRET64 simplifies the code, allowing CLEAR_CPU_BUFFERS to be explicitly added to syscall_return_via_sysret path. Below is with CONFIG_PARAVIRT_XXL=y and this patch applied: syscall_return_via_sysret: ... <+342>: swapgs <+345>: xchg %ax,%ax <+347>: verw -0x1a2(%rip) <------ <+354>: sysretq]	2024-06-25	8.8	High
CVE-2024-29176	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a buffer overflow vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to an application crash or execution of arbitrary code on the vulnerable application's underlying operating system with privileges of the vulnerable application.	2024-06-26	8.8	High
CVE-2024-37140	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an OS command injection vulnerability in an admin operation. A remote low privileged	2024-06-26	8.8	High

		attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the system application's underlying OS with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.			
CVE-2024-38384	Linux	In the Linux kernel, the following vulnerability has been resolved: blk-cgroup: fix list corruption from reorder of WRITE ->lqueued __blkcg_rstat_flush() can be run anytime, especially when blk_cgroup_bio_start is being executed. If WRITE of `->lqueued` is re-ordered with READ of 'bisc->lnode.next' in the loop of __blkcg_rstat_flush(), `next_bisc` can be assigned with one stat instance being added in blk_cgroup_bio_start(), then the local list in __blkcg_rstat_flush() could be corrupted. Fix the issue by adding one barrier.	2024-06-24	8.4	High
CVE-2023-30997	IBM	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254638.	2024-06-27	8.4	High
CVE-2023-30998	IBM	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254649.	2024-06-27	8.4	High
CVE-2024-35260	Microsoft	An authenticated attacker can exploit an Untrusted Search Path vulnerability in Microsoft Dataverse to execute code over a network.	2024-06-27	8	High
CVE-2024-38664	Linux	In the Linux kernel, the following vulnerability has been resolved: drm: zynqmp_dpsub: Always register bridge We must always register the DRM bridge, since zynqmp_dp_hpd_work_func calls drm_bridge_hpd_notify, which in turn expects hpd_mutex to be initialized. We do this before zynqmp_dpsub_drm_init since that calls drm_bridge_attach. This fixes the following lockdep warning: [19.217084] ------------[cut here]------------ [19.227530] DEBUG_LOCKS_WARN_ON(lock->magic != lock) [19.227768] WARNING: CPU: 0 PID: 140 at kernel/locking/mutex.c:582 __mutex_lock+0x4bc/0x550 [19.241696] Modules linked in: [19.244937] CPU: 0 PID: 140 Comm: kworker/0:4 Not tainted 6.6.20+ #96 [19.252046] Hardware name: xlnx,zynqmp (DT) [19.256421] Workqueue: events zynqmp_dp_hpd_work_func [19.261795] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [19.269104] pc : __mutex_lock+0x4bc/0x550 [19.273364] lr : __mutex_lock+0x4bc/0x550 [19.277592] sp : ffffffc085c5bbe0 [19.281066] x29: ffffffc085c5bbe0 x28: 0000000000000000 x27: ffffff88009417f8 [19.288624] x26: ffffff8800941788 x25: ffffff8800020008 x24: ffffffc082aa3000 [19.296227] x23: ffffffc080d90e3c x22: 0000000000000002 x21: 0000000000000000 [19.303744] x20: 0000000000000000 x19: ffffff88002f5210 x18: 0000000000000000 [19.311295] x17: 6c707369642e3030 x16: 3030613464662072 x15: 0720072007200720 [19.318922] x14: 0000000000000000 x13: 284e4f5f4e524157 x12: 0000000000000001 [19.326442] x11: 0001ffc085c5b940 x10: 0001ff88003f388b x9 : 0001ff88003f3888 [19.334003] x8 : 0001ff88003f3888 x7 : 0000000000000000 x6 : 0000000000000000 [19.341537] x5 : 0000000000000000 x4 : 0000000000001668 x3 : 0000000000000000 [19.349054] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffffff88003f3880 [19.356581] Call trace: [19.359160] __mutex_lock+0x4bc/0x550 [19.363032] mutex_lock_nested+0x24/0x30 [19.367187] drm_bridge_hpd_notify+0x2c/0x6c [19.371698] zynqmp_dp_hpd_work_func+0x44/0x54	2024-06-24	7.8	High

		[19.376364] process_one_work+0x3ac/0x988 [19.380660] worker_thread+0x398/0x694 [19.384736] kthread+0x1bc/0x1c0 [19.388241] ret_from_fork+0x10/0x20 [19.392031] irq event stamp: 183 [19.395450] hardirqs last enabled at (183): [<ffffffc0800b9278>] finish_task_switch.isra.0+0xa8/0x2d4 [19.405140] hardirqs last disabled at (182): [<ffffffc081ad3754>] __schedule+0x714/0xd04 [19.413612] softirqs last enabled at (114): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.423128] softirqs last disabled at (110): [<ffffffc080133de8>] srcu_invoke_callbacks+0x158/0x23c [19.432614] ---[end trace 0000000000000000]--- (cherry picked from commit 61ba791c4a7a09a370c45b70a81b8c7d4cf6b2ae)			
CVE-2024-38667	Linux	In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should be reserved for pt_regs. However this is not the case for the idle threads of the secondary boot harts. Their stacks overlap with their pt_regs, so both may get corrupted. Similar issue has been fixed for the primary hart, see c7cdd96eca28 ("riscv: prevent stack corruption by reserving task_pt_regs(p) early"). However that fix was not propagated to the secondary harts. The problem has been noticed in some CPU hotplug tests with V enabled. The function smp_callin stored several registers on stack, corrupting top of pt_regs structure including status field. As a result, kernel attempted to save or restore inexistent V context.	2024-06-24	7.8	High
CVE-2024-39291	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix buffer size in gfx_v9_4_3_init_ cp_compute_microcode() and rlc_microcode() The function gfx_v9_4_3_init_microcode in gfx_v9_4_3.c was generating about potential truncation of output when using the snprintf function. The issue was due to the size of the buffer 'ucode_prefix' being too small to accommodate the maximum possible length of the string being written into it. The string being written is "amdgpu/%s_mec.bin" or "amdgpu/%s_rlc.bin", where %s is replaced by the value of 'chip_name'. The length of this string without the %s is 16 characters. The warning message indicated that 'chip_name' could be up to 29 characters long, resulting in a total of 45 characters, which exceeds the buffer size of 30 characters. To resolve this issue, the size of the 'ucode_prefix' buffer has been reduced from 30 to 15. This ensures that the maximum possible length of the string being written into the buffer will not exceed its size, thus preventing potential buffer overflow and truncation issues. Fixes the below with gcc W=1: drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c: In function ‘gfx_v9_4_3_early_init’: drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:52: warning: ‘%s’ directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=] 379	snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name); | ^~	2024-06-24	7.8	High

<table>
<tr><td></td><td></td><td>......
 439 | r = gfx_v9_4_3_init_rlc_microcode(adev, ucode_prefix);
      | ~~~~~~~~~~~~
drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:379:9: note: ‘snprintf’ output between 16 and 45 bytes into a destination of size 30
 379 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_rlc.bin", chip_name);
      |
^~~~~~~
drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:52: warning: ‘%s’ directive output may be truncated writing up to 29 bytes into a region of size 23 [-Wformat-truncation=]
 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name);
      | ^~
......
 443 | r = gfx_v9_4_3_init_cp_compute_microcode(adev, ucode_prefix);
      | ~~~~~~~~~~~~
drivers/gpu/drm/amd/amdgpu/gfx_v9_4_3.c:413:9: note: ‘snprintf’ output between 16 and 45 bytes into a destination of size 30
 413 | snprintf(fw_name, sizeof(fw_name), "amdgpu/%s_mec.bin", chip_name);
      |
^~~~~~~</td><td></td><td></td><td></td></tr>
<tr><td>CVE-2024-22232</td><td>VMware</td><td>A specially crafted url can be created which leads to a directory traversal in the salt file server.
A malicious user can read an arbitrary file from a Salt master’s filesystem.</td><td>6/27/2024</td><td>7.7</td><td>High</td></tr>
<tr><td>CVE-2024-25943</td><td>Dell</td><td>iDRAC9, versions prior to 7.00.00.172 for 14th Generation and 7.10.50.00 for 15th and 16th Generations, contains a session hijacking vulnerability in IPMI. A remote attacker could potentially exploit this vulnerability, leading to arbitrary code execution on the vulnerable application.</td><td>2024-06-29</td><td>7.6</td><td>High</td></tr>
<tr><td>CVE-2024-6290</td><td>Google</td><td>Use after free in Dawn in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)</td><td>2024-06-24</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-6291</td><td>Google</td><td>Use after free in Swiftshader in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)</td><td>2024-06-24</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-6292</td><td>Google</td><td>Use after free in Dawn in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)</td><td>2024-06-24</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-6293</td><td>Google</td><td>Use after free in Dawn in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)</td><td>2024-06-24</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-31916</td><td>IBM</td><td>IBM OpenBMC FW1050.00 through FW1050.10 BMCWeb HTTPS server component could disclose sensitive URI content to an unauthorized actor that bypasses authentication channels. IBM X-ForceID: 290026.</td><td>2024-06-27</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2023-38370</td><td>IBM</td><td>IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1, under certain configurations, could allow a user on the network to install malicious packages. IBM X-Force ID: 261197.</td><td>2024-06-27</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-39348</td><td>Synology</td><td>Download of code without integrity check vulnerability in AirPrint functionality in Synology Router Manager (SRM) before 1.2.5-8227-11 and 1.3.1-9346-8 allows man-in-the-middle attackers to execute arbitrary code via unspecified vectors.</td><td>2024-06-28</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-39350</td><td>Synology</td><td>A vulnerability regarding authentication bypass by spoofing is found in the RTSP functionality. This allows man-in-the-middle attackers to obtain privileges without consent via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.</td><td>2024-06-28</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-31912</td><td>IBM</td><td>IBM MQ 9.3 LTS and 9.3 CD could allow an authenticated user to escalate their privileges under certain configurations due to incorrect privilege assignment. IBM X-Force ID: 289894.</td><td>2024-06-28</td><td>7.5</td><td>High</td></tr>
<tr><td>CVE-2024-21827</td><td>Tp-Link</td><td>A leftover debug code vulnerability exists in the cli_server debug functionality of Tp-Link ER7206 Omada Gigabit VPN Router 1.4.1 Build 20240117 Rel.57421. A specially crafted series of network requests can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.</td><td>2024-06-25</td><td>7.2</td><td>High</td></tr>
<tr><td>CVE-2023-47802</td><td>Synology</td><td>A vulnerability regarding improper neutralization of special elements used in an OS command ('OS Command Injection') is found in the IP block functionality. This allows remote</td><td>2024-06-28</td><td>7.2</td><td>High</td></tr>
</table>

		authenticated users with administrator privileges to execute arbitrary commands via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.			
CVE-2024-39351	Synology	A vulnerability regarding improper neutralization of special elements used in an OS command ('OS Command Injection') is found in the NTP configuration. This allows remote authenticated users with administrator privileges to execute arbitrary commands via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	7.2	High
CVE-2024-38272	Google	There exists a vulnerability in Quickshare/Nearby where an attacker can bypass the accept file dialog on QuickShare Windows. Normally in QuickShare Windows app we can't send a file without the user accept from the receiving device if the visibility is set to everyone mode or contacts mode. We recommend upgrading to version 1.0.1724.0 of Quickshare or above	2024-06-26	7.1	High
CVE-2024-29173	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a Server-Side Request Forgery (SSRF) vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to disclosure of information on the application or remote client.	2024-06-26	6.8	Medium
CVE-2024-37139	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an Improper Control of a Resource Through its Lifetime vulnerability in an admin operation. A remote low privileged attacker could potentially exploit this vulnerability, leading to temporary resource constraint of system application. Exploitation may lead to denial of service of the application.	2024-06-26	6.5	Medium
CVE-2024-35155	IBM	IBM MQ Console 9.3 LTS and 9.3 CD could disclose could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 292765.	2024-06-28	6.5	Medium
CVE-2024-25031	IBM	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.4 uses an inadequate account lockout setting that could allow an attacker on the network to brute force account credentials. IBM X-Force ID: 281678.	2024-06-28	6.5	Medium
CVE-2024-35156	IBM	IBM MQ 9.3 LTS and 9.3 CD could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 292766.	2024-06-28	6.5	Medium
CVE-2024-36038	ManageEngine	Zoho ManageEngine ITOM products versions from 128234 to 128248 are affected by the stored cross-site scripting vulnerability in the proxy server option.	2024-06-24	6.3	Medium
CVE-2023-30430	IBM	IBM Security Verify Access 10.0.0 through 10.0.7.1 could allow a local user to obtain sensitive information from trace logs. IBM X-Force ID: 252183.	2024-06-27	6.2	Medium
CVE-2023-38368	IBM	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could disclose sensitive information to a local user to do improper permission controls. IBM X-Force ID: 261195.	2024-06-27	6.2	Medium
CVE-2024-35137	IBM	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to possibly elevate their privileges due to sensitive configuration information being exposed. IBM X-Force ID: 292413.	2024-06-28	6.2	Medium
CVE-2024-35139	IBM	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain sensitive information from the container due to incorrect default permissions. IBM X-Force ID: 292415.	2024-06-28	6.2	Medium
CVE-2024-28973	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a Stored Cross-Site Scripting Vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a high privileged victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery	2024-06-26	5.9	Medium
CVE-2024-29175	Dell	Dell PowerProtect Data Domain, versions prior to 7.13.0.0, LTS 7.7.5.40, LTS 7.10.1.30 contain an weak cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to man-in-the-middle attack that exposes sensitive session information.	2024-06-26	5.9	Medium
CVE-2024-38271	Google	There exists a vulnerability in Quickshare/Nearby where an attacker can force the a victim to stay connected to a temporary hotspot created for the share. As part of the sequence of packets in a QuickShare connection over Bluetooth, the attacker forces the	2024-06-26	5.9	Medium

		victim to connect to the attacker's WiFi network and then sends an OfflineFrame that crashes Quick Share. This makes the Wifi connection to the attacker's network last instead of returning to the old network when the Quick Share session is done allowing the attacker to be a MiTM. We recommend upgrading to version 1.0.1724.0 of Quickshare or above			
CVE-2023-38371	IBM	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 261198.	2024-06-27	5.9	Medium
CVE-2024-39347	Synology	Incorrect default permissions vulnerability in firewall functionality in Synology Router Manager (SRM) before 1.2.5-8227-11 and 1.3.1-9346-8 allows man-in-the-middle attackers to access highly sensitive intranet resources via unspecified vectors.	2024-06-28	5.9	Medium
CVE-2024-31919	IBM	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS and 9.3 CD, in certain configurations, is vulnerable to a denial of service attack caused by an error processing messages when an API Exit using MQBUFMH is used. IBM X-Force ID: 290259.	2024-06-28	5.9	Medium
CVE-2024-25053	IBM	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, and 12.0.2 is vulnerable to improper certificate validation when using the IBM Planning Analytics Data Source Connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between IBM Planning Analytics server and IBM Cognos Analytics server. IBM X-Force ID: 283364.	2024-06-28	5.9	Medium
CVE-2024-35116	IBM	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, and 9.3 CD is vulnerable to a denial of service attack caused by an error applying configuration changes. IBM X-Force ID: 290335.	2024-06-28	5.9	Medium
CVE-2024-39292	Linux	In the Linux kernel, the following vulnerability has been resolved: um: Add winch to winch_handlers before registering winch IRQ Registering a winch IRQ is racy, an interrupt may occur before the winch is added to the winch_handlers list. If that happens, register_winch_irq() adds to that list a winch that is scheduled to be (or has already been) freed, causing a panic later in winch_cleanup(). Avoid the race by adding the winch to the winch_handlers list before registering the IRQ, and rolling back if um_request_irq() fails.	2024-06-24	5.5	Medium
CVE-2024-34141	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-06-25	5.4	Medium
CVE-2024-34142	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-06-25	5.4	Medium
CVE-2023-42014	IBM	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.2.0.2 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user 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: 265511.	2024-06-27	5.4	Medium
CVE-2024-25041	IBM	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, and 12.0.2 is potentially vulnerable to cross site scripting (XSS). A remote attacker could execute malicious commands due to improper validation of column headings in Cognos Assistant. IBM X-Force ID: 282780.	2024-06-28	5.4	Medium
CVE-2024-0171	Dell	Dell PowerEdge Server BIOS contains an TOCTOU race condition vulnerability. A local low privileged attacker could potentially exploit this vulnerability to gain access to otherwise unauthorized resources.	2024-06-25	5.3	Medium
CVE-2024-31883	IBM	IBM Security Verify Access 10.0.0.0 through 10.0.7.1, under certain configurations, could allow an unauthenticated attacker to cause a denial of service due to asymmetric resource consumption. IBM X-Force ID: 287615.	2024-06-27	5.3	Medium
CVE-2023-47803	Synology	A vulnerability regarding improper limitation of a pathname to a restricted directory ('Path Traversal') is found in the Language Settings functionality. This allows remote attackers to read specific	2024-06-28	5.3	Medium

		files containing non-sensitive information via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.			
CVE-2024-38322	IBM	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.4 agent username and password error response discrepancy exposes product to brute force enumeration. IBM X-Force ID: 294869.	2024-06-28	5.3	Medium
CVE-2024-22231	VMware	Syndic cache directory creation is vulnerable to a directory traversal attack in salt project which can lead a malicious attacker to create an arbitrary directory on a Salt master.	2024-06-27	5	Medium
CVE-2024-39352	Synology	A vulnerability regarding incorrect authorization is found in the firmware upgrade functionality. This allows remote authenticated users with administrator privileges to bypass firmware integrity check via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	2024-06-28	4.9	Medium
CVE-2024-35153	IBM	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows a privileged user 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: 292640.	2024-06-27	4.8	Medium
CVE-2024-29174	Dell	Dell Data Domain, versions prior to 7.13.0.0, LTS 7.7.5.30, LTS 7.10.1.20 contain an SQL Injection vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing unauthorized access to application data.	2024-06-26	4.4	Medium
CVE-2023-42011	IBM	IBM Sterling B2B Integrator Standard Edition 6.1 and 6.2 does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with. IBM X-Force ID: 265508.	2024-06-27	4.3	Medium
CVE-2024-37138	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 on DDMC contain a relative path traversal vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the application sending over an unauthorized file to the managed system.	2024-06-26	4.1	Medium
CVE-2022-38383	IBM	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Software Suite 1.10.12.0 through 1.10.21.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 233673.	2024-06-28	4	Medium
CVE-2024-32855	Dell	Dell Client Platform BIOS contains an Out-of-bounds Write vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	2024-06-25	3.8	Low
CVE-2024-37137	Dell	Dell Key Trust Platform, v3.0.6 and prior, contains Use of a Cryptographic Primitive with a Risky Implementation vulnerability. A local privileged attacker could potentially exploit this vulnerability, leading to privileged information disclosure.	2024-06-28	3.8	Low
CVE-2024-37141	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an open redirect vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-06-26	3.5	Low
CVE-2024-29177	Dell	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a disclosure of temporary sensitive information vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the reuse of disclosed information to gain unauthorized access to the application report.	2024-06-26	2.7	Low