https://nciipc.gov.in/

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16-31 May 2024 Vol. 11 No. 10

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Checkpoint					
Product: cloudguard_network_security					
Affected Version(s): r80.40					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**	https://support.checkpoint.com/results/sk/sk182336	A-CHE-CLOU-050624/1
Affected Version(s): r81.0					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates	https://support.checkpoint.com/results/sk/sk182336	A-CHE-CLOU-050624/2

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability is available. **CVE ID: CVE-2024-24919**		
Affected Version(s): r81.10					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**	https://support.checkpoint.com/results/sk/sk182336	A-CHE-CLOU-050624/3
Affected Version(s): r81.20					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available.	https://support.checkpoint.com/results/sk/sk182336	A-CHE-CLOU-050624/4

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-24919		
Vendor: Cisco					
Product: firepower_management_center					
Affected Version(s): From (including) 7.0.0 Up to (including) 7.3.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-May-2024	8.8	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs	A-CIS-FIRE-050624/5

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system, and elevate privileges to root. To exploit this vulnerability, an attacker would need at least Read Only user credentials. **CVE ID: CVE-2024-20360**		
Vendor: cloudwise					
Product: flyfish					
Affected Version(s): 3.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-May-2024	7.5	FlyFish v3.0.0 was discovered to contain a buffer overflow via the password parameter on the login page. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input. **CVE ID: CVE-2024-34905**	N/A	A-CLO-FLYF-050624/6
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 125.0.6422.112					
Access of Resource Using Incompatible Type ('Type Confusion')	28-May-2024	8.8	Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a	https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-050624/7

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandbox via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-5274**		
Vendor: ivanti					
Product: endpoint_manager_mobile					
Affected Version(s): * Up to (excluding) 12.1.0.0					
N/A	22-May-2024	6.7	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. **CVE ID: CVE-2024-22026**	https://forums.ivanti.com/s/article/Security-Advisory-EPMM-May-2024?language=en_US	A-IVA-ENDP-050624/8
Vendor: javs					
Product: javs_viewer					
Affected Version(s): 8.3.7.250					
N/A	23-May-2024	8.4	Justice AV Solutions Viewer Setup 8.3.7.250-1 contains a malicious binary when executed and is signed with an unexpected authenticode signature. A remote, privileged threat actor may exploit this	https://www.javs.com/downloads/	A-JAV-JAVS-050624/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute of unauthorized PowerShell commands. **CVE ID: CVE-2024-4978**		
Hardware					
Vendor: Checkpoint					
Product: quantum_security_gateway					
Affected Version(s): -					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**	https://support.checkpoint.com/results/sk/sk182336	H-CHE-QUAN-050624/10
Product: quantum_spark					
Affected Version(s): -					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to	https://support.checkpoint.com/results/sk/sk182336	H-CHE-QUAN-050624/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**		
Operating System					
Vendor: Checkpoint					
Product: quantum_security_gateway_firmware					
Affected Version(s): r80.40					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**	https://support.checkpoint.com/results/sk/sk182336	O-CHE-QUAN-050624/12
Affected Version(s): r81.0					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point	https://support.checkpoint.com/results/sk/sk182336	O-CHE-QUAN-050624/13

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**		
Affected Version(s): r81.10					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**	https://support.checkpoint.com/results/sk/sk182336	O-CHE-QUAN-050624/14
Affected Version(s): r81.20					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to	https://support.checkpoint.com/results/sk/sk182336	O-CHE-QUAN-050624/15

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**		
Product: quantum_spark_firmware					
Affected Version(s): r81.10					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**	https://support.checkpoint.com/results/sk/sk182336	O-CHE-QUAN-050624/16
Affected Version(s): r80.20					
N/A	28-May-2024	8.6	Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and	https://support.checkpoint.com/results/sk/sk182336	O-CHE-QUAN-050624/17

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available. **CVE ID: CVE-2024-24919**		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 4.14.331					
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42fda2d486f67745d7, https://git.kernel.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	O-LIN-LINU-050624/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code-loading, such scenario ends with null-ptr-deref. **CVE ID: CVE-2023-52806**		
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52809**	https://git.kernel.org/stable/c/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495ebecbb9395101f3be177cd0a52450b	O-LIN-LINU-050624/19
Affected Version(s): * Up to (excluding) 4.19.300					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52753**	https://git.kernel.org/stable/c/09909f515032fa80b921fd3118efe66b185d10fd, https://git.kernel.org/stable/c/4e497f1acd99075b13605b2e7fa0cba721a2cfd9, https://git.kernel.org/stable/c/6d8653b1a7a8dc938b566ae8c4f373b36e792c68	O-LIN-LINU-050624/20
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: 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	https://git.kernel.org/stable/c/174f62a0aa15c211e60208b41ee9e7cdfb73d455, https://git.kernel.org/stable/c/437e0fa907ba39b4d7eda863c03ea9cf48bd93a9, https://git.kernel.org/stable/c/5104fdf50d326db2c1a994f8b35dcd46e63ae4ad	O-LIN-LINU-050624/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 0xfffffffffffffd6. [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: 0000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00 R12: 00007f5e067530 00 [4005007.702618] R13: ffff9940656e0000 R14: ffffa82b46d27e68 R15: 00007f5e067530 00 [4005007.702622] FS: 00007f5e0755b7 40(0000) GS:ffff99479d300 000(0000) knlGS:000000000 0000000 [4005007.702626] CS: 0010 DS: 0000 ES: 0000 CR0: 00000000800500 33 [4005007.702629] CR2: fffffffffffffd6 CR3: 00000003253fc00 0 CR4: 00000000003506 e0 [4005007.702633] Call Trace: [4005007.702636] <TASK> [4005007.702640] amdgpu_debugfs_ regs_smc_read+0x		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			b0/0x120 [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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			binfmt_misc nls_iso8859_1 ipmi_ssif ast intel_rapl_msr intel_rapl_common drm_vram_helper drm_ttm_helper amd64_edac tm edac_mce_amd kvm_amd ccp mac_hid k10temp kvm acpi_ipmi ipmi_si rapl sch_fq_codel ipmi_devintf ipmi_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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xhci_pci_renesas dca [4005007.703184] CR2: 0000000000000000 [4005007.703188] ---[en ---truncated--- **CVE ID: CVE-2023-52817**		
Affected Version(s): * Up to (excluding) 5.10.202					
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52814**	https://git.kernel.org/stable/c/80285ae1ec8717b597b20de38866c29d84d321a1, https://git.kernel.org/stable/c/9b70fc7d70e8ef7c4a65034c9487f58609e708a1, https://git.kernel.org/stable/c/b0702ee4d811708251cdf54d4a1d3e888d365111	O-LIN-LINU-050624/22
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2381f6b628b3214f07375e0adf5ce17093c31190, https://git.kern	O-LIN-LINU-050624/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52821**	el.org/stable/c/4fa930ba046d20fc1899770396ee11e905fa96e4, https://git.kernel.org/stable/c/79813cd59398015867d51e6d7dcc14d287d4c402	
Affected Version(s): * Up to (excluding) 5.15.140					
NULL Pointer Dereference	21-May-2024	5.5	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()	https://git.kernel.org/stable/c/33fb1a555354bd593f785935ddcb5d9dd4d3847f, https://git.kernel.org/stable/c/70f831f21155c692bb336c434936fd6f24f3f81a, https://git.kernel.org/stable/c/8c6c85a073768df68c1a3fea143d013a38c66d34	O-LIN-LINU-050624/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52815**		
Affected Version(s): * Up to (excluding) 6.1.64					
Use After Free	21-May-2024	7.8	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	https://git.kernel.org/stable/c/0ab6f842452ce2cae04209d4671ac6289d0aef8a, https://git.kernel.org/stable/c/558817597d5fbd7af31f891b67b0fd20f0d047b7, https://git.kernel.org/stable/c/89929ea46f9cc11ba66d2c64713aa5d5dc723b09	O-LIN-LINU-050624/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/proc/fs/cifs/DebugData while mounting and umounting [816.251274] general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b6b6d81: 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_p		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			roc_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 **CVE ID: CVE-2023-52752**		
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/3a23b384e7e3d64d5587ad10729a34d4f761517e, https://git.kern	O-LIN-LINU-050624/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 **CVE ID: CVE-2023-52802**	el.org/stable/c/5b82e4240533bcd4691e50b64ec86d0d7fbd21b9, https://git.kernel.org/stable/c/b028f89c56e964a22d3ddb8eab1a0e7e980841b9	
Affected Version(s): * Up to (excluding) 6.5.13					
Out-of-bounds Read	21-May-2024	7.1	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	https://git.kernel.org/stable/c/1bc44a505a229bb1dd4957e11aa594edeea3690e, https://git.kernel.org/stable/c/79527c21a3ce04cffc35ea54f74ee087e532be57, https://git.kernel.org/stable/c/c9e44111da221246efb2e623	O-LIN-LINU-050624/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52827**	ae1be40a5cf6542c	
Affected Version(s): * Up to (excluding) 6.6.3					
Use After Free	21-May-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix slab-use-after-free in gfs2_qd_dealloc	https://git.kernel.org/stable/c/08a28272faa750d4357ea2cb48d2baefd778ea81, https://git.kernel.org/stable/c/bdcb8aa434c6d36b5c215d02a9ef07551be25a37	O-LIN-LINU-050624/28

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52760**		
Affected Version(s): From (including) 3.13 Up to (excluding) 4.19.313					
Loop with Unreachabl	20-May-2024	5.5	In the Linux kernel, the	https://git.kernel.org/stable/c	O-LIN-LINU-050624/29

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
e Exit Condition ('Infinite Loop')			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	/04720ea2e6c64459a90ca28570ea78335eccd924, https://git.kernel.org/stable/c/3fe79b2c83461edbbf86ed8a6f3924820ff89259, https://git.kernel.org/stable/c/4ca2a5fb54ea2cc43edea614207fcede562d91c2	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(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 ID: CVE-2024-35982**		
Affected Version(s): From (including) 3.19 Up to (excluding) 4.19.313					
NULL Pointer Dereference	20-May-2024	5.5	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	https://git.kernel.org/stable/c/357c64ef1ef39b1e7cd91ab6bdd304d043702c83, https://git.kernel.org/stable/c/40f1d79f07b49c8a64a861706e5163f2db4bd95d, https://git.kernel.org/stable/c/4e75e222d397c6752b229ed72fc4644c8c36ecde	O-LIN-LINU-050624/30

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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] **CVE ID: CVE-2024-35984**		
Affected Version(s): From (including) 3.8 Up to (excluding) 4.19.313					
Improper Locking	20-May-2024	5.5	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. However, this is not necessary, because I2C core already has its own	https://git.kernel.org/stable/c/0561b65fbd53d3e788c5b0222d9112ca016fd6a1, https://git.kernel.org/stable/c/21bfca822cfc1e71796124e93b46e0d9fa584401, https://git.kernel.org/stable/c/29e94f295bad5be59cf4271a93e22cdcf5536722	O-LIN-LINU-050624/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35997**		
Affected Version(s): From (including) 4.1 Up to (excluding) 4.19.313					
Missing Release of Memory after	20-May-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/45d355a926ab40f3ae7bc0b0	O-LIN-LINU-050624/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			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. **CVE ID: CVE-2024-35978**	a00cb0e3e8a5a810, https://git.kernel.org/stable/c/4beab84fbb50df3be1d8f8a976e6fe882ca65cb2, https://git.kernel.org/stable/c/66fab1e120b39f8f47a94186ddee36006fc02ca8	
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.300					
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42fda2d486f67745d7, https://git.kernel.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	O-LIN-LINU-050624/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52806**		
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495ebecbb9395101f3be177cd0a52450b	O-LIN-LINU-050624/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message on fc_rport_create() failed. **CVE ID: CVE-2023-52809**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.262					
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52753**	https://git.kernel.org/stable/c/09909f515032fa80b921fd3118efe66b185d10fd, https://git.kernel.org/stable/c/4e497f1acd99075b13605b2e7fa0cba721a2cfd9, https://git.kernel.org/stable/c/6d8653b1a7a8dc938b566ae8c4f373b36e792c68	O-LIN-LINU-050624/35
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: Fix possible null-ptr-deref when assigning a stream	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42fda2d486f67745d7, https://git.kern	O-LIN-LINU-050624/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52806**	el.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495ebecbb9395101f3be177cd0a52450b	O-LIN-LINU-050624/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference. Address this issue by checking return value of fc_rport_create() and log error message on fc_rport_create() failed. **CVE ID: CVE-2023-52809**		
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: 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:	https://git.kernel.org/stable/c/174f62a0aa15c211e60208b41ee9e7cdfb73d455, https://git.kernel.org/stable/c/437e0fa907ba39b4d7eda863c03ea9cf48bd93a9, https://git.kernel.org/stable/c/5104fdf50d326db2c1a994f8b35dcd46e63ae4ad	O-LIN-LINU-050624/38

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 00007f5e0675300 [4005007.702618] R13: ffff9940656e0000 R14: ffffa82b46d27e68 R15:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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_6		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4_after_hwframe+ 0x44/0xae [4005007.703075] RIP: 0033:0x7f5e0767 2992 [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:00007ffe03 097898 EFLAGS: 00000246 ORIG_RAX: 00000000000000 00 [4005007.703088] RAX: ffffffffffffffda RBX: 00000000000200 00 RCX: 00007f5e076729 92 [4005007.703091] RDX: 00000000000200 00 RSI: 00007f5e067530 00 RDI: 00000000000000 03		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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 ttm edac_mce_amd kvm_amd ccp		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mac_hid k10temp kvm acpi_ipmi ipmi_si rapl sch_fq_codel ipmi_devintf ipmi_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---		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-52817		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.275					
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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. **CVE ID: CVE-2024-35978**	https://git.kernel.org/stable/c/45d355a926ab40f3ae7bc0b0a00cb0e3e8a5a810, https://git.kernel.org/stable/c/4beab84fbb50df3be1d8f8a976e6fe882ca65cb2, https://git.kernel.org/stable/c/66fab1e120b39f8f47a94186ddee36006fc02ca8	O-LIN-LINU-050624/39
Loop with Unreachable Exit Condition ('Infinite Loop')	20-May-2024	5.5	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	https://git.kernel.org/stable/c/04720ea2e6c64459a90ca28570ea78335eccd924, https://git.kernel.org/stable/c/3fe79b2c83461edbbf86ed8a6f3924820ff89259, https://git.kernel.org/stable/c/4ca2a5fb54ea2cc43edea6142	O-LIN-LINU-050624/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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)	07fcede562d91c2	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. 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:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incompatible system configuration are present. **CVE ID: CVE-2024-35982**		
NULL Pointer Dereference	20-May-2024	5.5	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]	https://git.kernel.org/stable/c/357c64ef1ef39b1e7cd91ab6bdd304d043702c83, https://git.kernel.org/stable/c/40f1d79f07b49c8a64a861706e5163f2db4bd95d, https://git.kernel.org/stable/c/4e75e222d397c6752b229ed72fc4644c8c36ecde	O-LIN-LINU-050624/41

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35984		
Improper Locking	20-May-2024	5.5	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. 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	https://git.kernel.org/stable/c/0561b65fbd53d3e788c5b0222d9112ca016fd6a1, https://git.kernel.org/stable/c/21bfca822cfc1e71796124e93b46e0d9fa584401, https://git.kernel.org/stable/c/29e94f295bad5be59cf4271a93e22cdcf5536722	O-LIN-LINU-050624/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35997**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.140					
NULL Pointer Dereference	21-May-2024	5.5	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.	https://git.kernel.org/stable/c/09909f515032fa80b921fd3118efe66b185d10fd, https://git.kernel.org/stable/c/4e497f1acd99075b13605b2e7fa0cba721a2cfd9, https://git.kernel.org/stable/c/6d8653b1a7a8dc938b566ae8c4f373b36e792c68	O-LIN-LINU-050624/43

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-52753		
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52806**	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42fda2d486f67745d7, https://git.kernel.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	O-LIN-LINU-050624/44
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c	O-LIN-LINU-050624/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52809**	/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495ebecbb9395101f3be177cd0a52450b	
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix potential null pointer derefernce The amdgpu_ras_get_c	https://git.kernel.org/stable/c/80285ae1ec8717b597b20de38866c29d84d321a1, https://git.kernel.org/stable/c/9b70fc7d70e8ef7c4a65034c9487f58609e708a1, https://git.kernel.org/stable/c/b0702ee4d81	O-LIN-LINU-050624/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ontext may return NULL if device not support ras feature, so add check before using. **CVE ID: CVE-2023-52814**	1708251cdf54d4a1d3e888d365111	
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: 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	https://git.kernel.org/stable/c/174f62a0aa15c211e60208b41ee9e7cdfb73d455, https://git.kernel.org/stable/c/437e0fa907ba39b4d7eda863c03ea9cf48bd93a9, https://git.kernel.org/stable/c/5104fdf50d326db2c1a994f8b35dcd46e63ae4ad	O-LIN-LINU-050624/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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:ffffa82b46d		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			27da0 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: 00007f5e067530 00 [4005007.702618] R13: ffff9940656e0000 R14: ffffa82b46d27e68 R15: 00007f5e067530 00 [4005007.702622] FS: 00007f5e0755b7		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			40(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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0033:0x7f5e0767 2992 [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:00007ffe03 097898 EFLAGS: 00000246 ORIG_RAX: 00000000000000 00 [4005007.703088] RAX: ffffffffffffffda RBX: 00000000000200 00 RCX: 00007f5e076729 92 [4005007.703091] RDX: 00000000000200 00 RSI: 00007f5e067530 00 RDI: 00000000000000 03 [4005007.703094] RBP: 00007f5e067530 00 R08: 00007f5e067520		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10 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 ttm edac_mce_amd kvm_amd ccp mac_hid k10temp kvm acpi_ipmi ipmi_si rapl sch_fq_codel ipmi_devintf ipm		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2023-52817**		
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/2381f6b628b3214f07375e0a	O-LIN-LINU-050624/48

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52821**	df5ce17093c31190, https://git.kernel.org/stable/c/4fa930ba046d20fc1899770396ee11e905fa96e4, https://git.kernel.org/stable/c/79813cd59398015867d51e6d7dcc14d287d4c402	
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.156					
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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	https://git.kernel.org/stable/c/45d355a926ab40f3ae7bc0b0a00cb0e3e8a5a810, https://git.kernel.org/stable/c/4beab84fbb50df3be1d8f8a976e6fe882ca65cb2, https://git.kernel.org/stable/c/66fab1e120b3	O-LIN-LINU-050624/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free the previous sync request state before assigning reference to a new one. **CVE ID: CVE-2024-35978**	9f8f47a94186ddee36006fc02ca8	
Loop with Unreachable Exit Condition ('Infinite Loop')	20-May-2024	5.5	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	https://git.kernel.org/stable/c/04720ea2e6c64459a90ca28570ea78335eccd924, https://git.kernel.org/stable/c/3fe79b2c83461edbbf86ed8a6f3924820ff89259, https://git.kernel.org/stable/c/4ca2a5fb54ea2cc43edea614207fcede562d91c2	O-LIN-LINU-050624/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. There are other scenarios possible with a similar result. The number of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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)		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35982**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.158					
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Fix possible memory leak in	https://git.kernel.org/stable/c/10a9d6a7513f93d7faffcb341af0aa42be8218fe, https://git.kernel.org/stable/c/7ac10c7d728d75bc9daaa8fade3c7a3273b9a	O-LIN-LINU-050624/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2024-35972**	9ff, https://git.kernel.org/stable/c/c60ed825530b8c0cc2b524efd39b1d696ec54004	
NULL Pointer Dereference	20-May-2024	5.5	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	https://git.kernel.org/stable/c/357c64ef1ef39b1e7cd91ab6bdd304d043702c83, https://git.kernel.org/stable/c/40f1d79f07b49c8a64a861706e5163f2db4bd95d, https://git.kernel.org/stable/c/4e75e222d397c6752b229ed72fc4644c8c36ecde	O-LIN-LINU-050624/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			always being available. Fix this by always checking the pointer in __i2c_transfer. [wsa: dropped the simplification in core-smbus to avoid theoretical regressions] **CVE ID: CVE-2024-35984**		
Improper Locking	20-May-2024	5.5	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	https://git.kernel.org/stable/c/0ccac964520a6f19e355652c8ca38af2a7f27076, https://git.kernel.org/stable/c/244296cc3a155199a8b080d19e645d7d49081a38, https://git.kernel.org/stable/c/8bf574183282d219cfa991f7df37aad491d74c11	O-LIN-LINU-050624/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 0000000000000001 [31.079613] x11: 0001ffc083bb2e34 x10: 0001ff880164e98		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f 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_helpe		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r_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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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_dr		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			m_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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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 ID: CVE-2024-35990**		
Improper Locking	20-May-2024	5.5	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	https://git.kernel.org/stable/c/0561b65fbd53d3e788c5b0222d9112ca016fd6a1, https://git.kernel.org/stable/c/21bfca822cfc1e71796124e93b46e0d9fa584401, https://git.kernel.org/stable/c/29e94f295bad5be59cf4271a9	O-LIN-LINU-050624/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			serialize I2C operations. 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.	3e22cdcf5536722	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35997		
NULL Pointer Dereference	20-May-2024	5.5	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	https://git.kernel.org/stable/c/03b5a9b2b526862b21bcc31976e393a6e63785d1, https://git.kernel.org/stable/c/58a4c9b1e5a3e53c9148e80b90e1e43897ce77d1, https://git.kernel.org/stable/c/7a25bfd12733a8f38f8ca47c581f876c3d481ac0	O-LIN-LINU-050624/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RCX: ffff88800f4f90c0 RDX: 0000000000000000 RSI: 0000000004001eac RDI: ffff8880160c64c0 RBP: ffffc900015ff060 R08: 0000000000000000 R09: ffff88800f7a4000 R10: 0000000000000002 R11: ffff88800f4f90c0 R12: dfffc0000000000 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:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 **CVE ID: CVE-2024-36008**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.140					
Use After Free	21-May-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: af_unix: fix use-after-free in unix_stream_read_actor()	https://git.kernel.org/stable/c/069a3ec329ff43e7869a3d94c62cd03203016bce, https://git.kernel.org/stable/c/4b7b492615cf3017190f55444f7016812b66	O-LIN-LINU-050624/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-	611d, https://git.kernel.org/stable/c/75bcfc188abf4fae9c1d5f5dc0a03540be602eef	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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+0 xd9/0x1b0 lib/dump_stack.c: 106 print_address_des cription mm/kasan/report .c:364 [inline] print_report+0xc4 /0x620 mm/kasan/report .c:475 kasan_report+0xd a/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+0x19a5/0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x2480 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 0000000000000001c RCX: 00007fc67492c559 RDX: 0000000040010083 RSI: 0000000020000140 RDI: 0000000000000004 RBP: 00007fc6749b6348 R08: 00007fc6748ab6c0 R09: 00007fc6748ab6c0 R10: 0000000000000000 R11: 0000000000000246 R12:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__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]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2023-52772**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.64					
Use After Free	21-May-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/069a3ec329ff43e7869a3d94c62cd0320301	O-LIN-LINU-050624/57

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: af_unix: fix use-after-free in unix_stream_read_actor() 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-	6bce, https://git.kernel.org/stable/c/4b7b492615cf3017190f55444f7016812b66611d, https://git.kernel.org/stable/c/75bcfc188abf4fae9c1d5f5dc0a03540be602eef	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 0000000000000001c RCX: 00007fc67492c559 RDX: 0000000040010083 RSI: 0000000020000140 RDI: 0000000000000004 RBP: 00007fc6749b6348 R08: 00007fc6748ab6c0 R09:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			___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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			___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---		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-52772		
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52753**	https://git.kernel.org/stable/c/09909f515032fa80b921fd3118efe66b185d10fd, https://git.kernel.org/stable/c/4e497f1acd99075b13605b2e7fa0cba721a2cfd9, https://git.kernel.org/stable/c/6d8653b1a7a8dc938b566ae8c4f373b36e792c68	O-LIN-LINU-050624/58
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42fda2d486f67745d7, https://git.kernel.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	O-LIN-LINU-050624/59

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52806**		
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495ebecbb9395101f3be177cd0a52450b	O-LIN-LINU-050624/60

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue by checking return value of fc_rport_create() and log error message on fc_rport_create() failed. **CVE ID: CVE-2023-52809**		
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52814**	https://git.kernel.org/stable/c/80285ae1ec8717b597b20de38866c29d84d321a1, https://git.kernel.org/stable/c/9b70fc7d70e8ef7c4a65034c9487f58609e708a1, https://git.kernel.org/stable/c/b0702ee4d811708251cdf54d4a1d3e888d365111	O-LIN-LINU-050624/61
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vkms: fix a possible	https://git.kernel.org/stable/c/33fb1a555354bd593f785935ddcb5d9dd4d3847f, https://git.kernel.org/stable/c/70f831f21155c692bb336c43	O-LIN-LINU-050624/62

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52815**	4936fd6f24f3f81a, https://git.kernel.org/stable/c/8c6c85a073768df68c1a3fea143d013a38c66d34	
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: 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	https://git.kernel.org/stable/c/174f62a0aa15c211e60208b41ee9e7cdfb73d455, https://git.kernel.org/stable/c/437e0fa907ba39b4d7eda863c03ea9cf48bd93a9, https://git.kernel.org/stable/c/5104fdf50d326db2c1a994f8b35dcd46e63ae4ad	O-LIN-LINU-050624/63

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 0xfffffffffffffd6. [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:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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] ?		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ec 28 48 89 54 24 [4005007.703083] RSP: 002b:00007ffe03097898 EFLAGS: 00000246 ORIG_RAX: 0000000000000000 [4005007.703088] RAX: ffffffffffffffda RBX: 0000000000020000 RCX: 00007f5e07672992		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ipmi_ssif ast intel_rapl_msr intel_rapl_commo n 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_help er(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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4005007.703184] CR2: 0000000000000000 [4005007.703188] ---[en ---truncated--- **CVE ID: CVE-2023-52817**		
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52821**	https://git.kernel.org/stable/c/2381f6b628b3214f07375e0adf5ce17093c31190, https://git.kernel.org/stable/c/4fa930ba046d20fc1899770396ee11e905fa96e4, https://git.kernel.org/stable/c/79813cd59398015867d51e6d7dcc14d287d4c402	O-LIN-LINU-050624/64
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.87					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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. **CVE ID: CVE-2024-35972**	https://git.kernel.org/stable/c/10a9d6a7513f93d7faffcb341af0aa42be8218fe, https://git.kernel.org/stable/c/7ac10c7d728d75bc9daaa8fade3c7a3273b9a9ff, https://git.kernel.org/stable/c/c60ed825530b8c0cc2b524efd39b1d696ec54004	O-LIN-LINU-050624/65
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix memory leak in hci_req_sync_complete() In 'hci_req_sync_com	https://git.kernel.org/stable/c/45d355a926ab40f3ae7bc0b0a00cb0e3e8a5a810, https://git.kernel.org/stable/c/4beab84fbb50df3be1d8f8a976e6fe882ca65cb2, https://git.kernel.org/stable/c	O-LIN-LINU-050624/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plete()', always free the previous sync request state before assigning reference to a new one. **CVE ID: CVE-2024-35978**	/66fab1e120b39f8f47a94186ddee36006fc02ca8	
Loop with Unreachable Exit Condition ('Infinite Loop')	20-May-2024	5.5	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	https://git.kernel.org/stable/c/04720ea2e6c64459a90ca28570ea78335eccd924, https://git.kernel.org/stable/c/3fe79b2c83461edbbf86ed8a6f3924820ff89259, https://git.kernel.org/stable/c/4ca2a5fb54ea2cc43edea614207fcede562d91c2	O-LIN-LINU-050624/67

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. There are other scenarios possible with a similar		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35982**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.90					
NULL Pointer Dereference	20-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: i2c: smbus: fix NULL function	https://git.kernel.org/stable/c/357c64ef1ef39b1e7cd91ab6bdd304d043702c83, https://git.kernel.org/stable/c/40f1d79f07b49c8a64a86170	O-LIN-LINU-050624/68

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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] **CVE ID: CVE-2024-35984**	6e5163f2db4bd95d, https://git.kernel.org/stable/c/4e75e222d397c6752b229ed72fc4644c8c36ecde	
Improper Locking	20-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma: xilinx_dpdma: Fix locking There are several places where either chan->lock	https://git.kernel.org/stable/c/0ccac964520a6f19e355652c8ca38af2a7f27076, https://git.kernel.org/stable/c/244296cc3a155199a8b080d19e645d7d49081a38, https://git.kernel.org/stable/c	O-LIN-LINU-050624/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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=--)	/8bf574183282d219cfa991f7df37aad491d74c11	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 [31.079453] x14: 0000000000000000 x13: ffffff8802263dc0 x12: 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 : 0000000000000c0 x0 : 0000000000000000 [31.080307] Call trace: [31.080340] xilinx_dpdma_chan_queue_transfer+0x274/0x5e0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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_modes		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			et_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_ini		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tial_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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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---		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35990		
Improper Locking	20-May-2024	5.5	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. 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	https://git.kernel.org/stable/c/0561b65fbd53d3e788c5b0222d9112ca016fd6a1, https://git.kernel.org/stable/c/21bfca822cfc1e71796124e93b46e0d9fa584401, https://git.kernel.org/stable/c/29e94f295bad5be59cf4271a93e22cdcf5536722	O-LIN-LINU-050624/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35997**		
NULL Pointer Dereference	20-May-2024	5.5	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].	https://git.kernel.org/stable/c/03b5a9b2b526862b21bcc31976e393a6e63785d1, https://git.kernel.org/stable/c/58a4c9b1e5a3e53c9148e80b90e1e43897ce77d1, https://git.kernel.org/stable/c/7a25bfd12733a8f38f8ca47c581f876c3d481ac0	O-LIN-LINU-050624/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 0xdffffc000000000: 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: dfffc0000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__se_sys_bpf kernel/bpf/syscall.c:5199 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5199 **CVE ID: CVE-2024-36008**		
Affected Version(s): From (including) 5.18 Up to (excluding) 6.1.90					
Out-of-bounds Read	20-May-2024	5.5	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.	https://git.kernel.org/stable/c/40406dfbc060503d2e0a9e637e98493c54997b3d, https://git.kernel.org/stable/c/610f175d2e16fb2436ba7974b990563002c20d07, https://git.kernel.org/stable/c/976df695f579bbb2914114b4e9974fe4ed1eb813	O-LIN-LINU-050624/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Found by Linux Verification Center (linuxtesting.org) with SVACE. **CVE ID: CVE-2024-35992**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.202					
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52753**	https://git.kernel.org/stable/c/09909f515032fa80b921fd3118efe66b185d10fd, https://git.kernel.org/stable/c/4e497f1acd99075b13605b2e7fa0cba721a2cfd9, https://git.kernel.org/stable/c/6d8653b1a7a8dc938b566ae8c4f373b36e792c68	O-LIN-LINU-050624/73
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: Fix possible null-ptr-	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42f	O-LIN-LINU-050624/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52806**	da2d486f67745d7, https://git.kernel.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	
NULL Pointer Dereference	21-May-2024	5.5	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()	https://git.kernel.org/stable/c/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495ebecbb9395101f3be177cd0a52450b	O-LIN-LINU-050624/75

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52809**		
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: 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	https://git.kernel.org/stable/c/174f62a0aa15c211e60208b41ee9e7cdfb73d455, https://git.kernel.org/stable/c/437e0fa907ba39b4d7eda863c03ea9cf48bd93a9, https://git.kernel.org/stable/c/5104fdf50d326db2c1a994f8b35dcd46e63ae4ad	O-LIN-LINU-050624/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4005007.702590] RIP: 0010:0x0 [4005007.702598] Code: Unable to access opcode bytes at RIP 0xfffffffffffffd6. [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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4005007.702618] R13: ffff9940656e0000 R14: ffffa82b46d27e68 R15: 0000 7f5e0675300 0 [4005007.702622] FS: 00007f5e0755b7 40(0000) GS:ffff99479d300 000(0000) knlGS:000000000 0000000 [4005007.702626] CS: 0010 DS: 0000 ES: 0000 CR0: 00000000800500 33 [4005007.702629] CR2: fffffffffffffd6 CR3: 00000003253fc00 0 CR4: 00000000003506 e0 [4005007.702633] Call Trace: [4005007.702636] <TASK> [4005007.702640] amdgpu_debugfs_ regs_smc_read+0x b0/0x120 [amdgpu] [4005007.703002]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4005007.703062] ? asm_exc_page_fault+0x8/0x30 [4005007.703068] entry_SYSCALL_64_after_hwframe+0x44/0xae [4005007.703075] RIP: 0033:0x7f5e076729 92 [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:00007ffe03 097898 EFLAGS: 00000246 ORIG_RAX: 00000000000000 00 [4005007.703088] RAX: ffffffffffffffda RBX: 00000000000200 00 RCX: 00007f5e076729 92 [4005007.703091] RDX:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intel_rapl_common drm_vram_helper drm_ttm_helper amd64_edac tm edac_mce_amd kvm_amd ccp mac_hid k10temp kvm acpi_ipmi ipmi_si rapl sch_fq_codel ipmi_devintf ipmi_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:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 [4005007.703188] ---[en ---truncated--- **CVE ID: CVE-2023-52817**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.216					
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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. **CVE ID: CVE-2024-35972**	https://git.kernel.org/stable/c/10a9d6a7513f93d7faffcb341af0aa42be8218fe, https://git.kernel.org/stable/c/7ac10c7d728d75bc9daaa8fade3c7a3273b9a9ff, https://git.kernel.org/stable/c/c60ed825530b8c0cc2b524efd39b1d696ec54004	O-LIN-LINU-050624/77
Missing Release of Memory after	20-May-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/45d355a926ab40f3ae7bc0b0a00cb0e3e8a5a	O-LIN-LINU-050624/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			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. **CVE ID: CVE-2024-35978**	810, https://git.kernel.org/stable/c/4beab84fbb50df3be1d8f8a976e6fe882ca65cb2, https://git.kernel.org/stable/c/66fab1e120b39f8f47a94186ddee36006fc02ca8	
Loop with Unreachable Exit Condition ('Infinite Loop')	20-May-2024	5.5	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	https://git.kernel.org/stable/c/04720ea2e6c64459a90ca28570ea78335eccd924, https://git.kernel.org/stable/c/3fe79b2c83461edbbf86ed8a6f3924820ff89259, https://git.kernel.org/stable/c/4ca2a5fb54ea2cc43edea614207fcede562d91c2	O-LIN-LINU-050624/79

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and will then stagnate at 0 and therefore never be able to reduce the table even more. 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 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 ID: CVE-2024-35982**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	20-May-2024	5.5	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] **CVE ID: CVE-2024-35984**	https://git.kernel.org/stable/c/357c64ef1ef39b1e7cd91ab6bdd304d043702c83, https://git.kernel.org/stable/c/40f1d79f07b49c8a64a861706e5163f2db4bd95d, https://git.kernel.org/stable/c/4e75e222d397c6752b229ed72fc4644c8c36ecde	O-LIN-LINU-050624/80
Improper Locking	20-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0561b65fbd53d3e788c5b0222d9112ca016f	O-LIN-LINU-050624/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. 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	d6a1, https://git.kernel.org/stable/c/21bfca822cfc1e71796124e93b46e0d9fa584401, https://git.kernel.org/stable/c/29e94f295bad5be59cf4271a93e22cdcf5536722	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35997**		
NULL Pointer Dereference	20-May-2024	5.5	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.	https://git.kernel.org/stable/c/03b5a9b2b526862b21bcc31976e393a6e63785d1, https://git.kernel.org/stable/c/58a4c9b1e5a3e53c9148e80b90e1e43897ce77d1, https://git.kernel.org/stable/c/7a25bfd12733a8f38f8ca47c581f876c3d481ac0	O-LIN-LINU-050624/82

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: dfffffc0000000000 R13: 0000000000000000 R14: 0000000000000000 R15: ffff88800f7a4000 FS: 00007f938acfe6c0(0000) GS:ffff888058c00000(0000)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 **CVE ID: CVE-2024-36008**		
Affected Version(s): From (including) 5.9 Up to (excluding) 5.10.216					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	20-May-2024	5.5	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	https://git.kernel.org/stable/c/0ccac964520a6f19e355652c8ca38af2a7f27076, https://git.kernel.org/stable/c/244296cc3a155199a8b080d19e645d7d49081a38, https://git.kernel.org/stable/c/8bf574183282d219cfa991f7df37aad491d74c11	O-LIN-LINU-050624/83

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[31.080147] x2 : ffffffc7f8d43000 x1 : 0000000000000c0 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[31.084932] irq event stamp: 64549 [31.084970] hardirqs last enabled at (64548): [<ffffffc081adf35c>] _raw_spin_unlock_irqrestore+0x80/0x90 [31.085157] ---truncated--- **CVE ID: CVE-2024-35990**		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.1.64					
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/1d07b7e84276777dad3c8cfebdf8e739606f90c9, https://git.kernel.org/stable/c/5b14cf37b9f01de0b28c6f8960019d4c7883ce42, https://git.kernel.org/stable/c/b71f4ade1b8900d30c661d6c27f87c35214c398c	O-LIN-LINU-050624/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52773**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.5.13					
Use After Free	21-May-2024	7.8	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.	https://git.kernel.org/stable/c/0ab6f842452ce2cae04209d4671ac6289d0aef8a, https://git.kernel.org/stable/c/558817597d5fbd7af31f891b67b0fd20f0d047b7, https://git.kernel.org/stable/c/89929ea46f9cc11ba66d2c64713aa5d5dc723b09	O-LIN-LINU-050624/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 0x6b6b6b6b6b6b6b6d81: 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]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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 **CVE ID: CVE-2023-52752**		
Use After Free	21-May-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/069a3ec329ff43e7869a3d94c62cd0320301	O-LIN-LINU-050624/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			af_unix: fix use-after-free in unix_stream_read_actor() 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	6bce, https://git.kernel.org/stable/c/4b7b492615cf3017190f55444f7016812b66611d, https://git.kernel.org/stable/c/75bcfc188abf4fae9c1d5f5dc0a03540be602eef	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 0000000000000001c RCX: 00007fc67492c559 RDX: 0000000040010083 RSI: 0000000020000140 RDI: 0000000000000004 RBP: 00007fc6749b6348 R08: 00007fc6748ab6c0 R09: 00007fc6748ab6c0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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+0x180/0x3		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c0 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			___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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2023-52772**		
NULL Pointer	21-May-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/09909f51503	O-LIN-LINU-050624/87

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			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. **CVE ID: CVE-2023-52753**	2fa80b921fd3118efe66b185d10fd, https://git.kernel.org/stable/c/4e497f1acd99075b13605b2e7fa0cba721a2cfd9, https://git.kernel.org/stable/c/6d8653b1a7a8dc938b566ae8c4f373b36e792c68	
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/1d07b7e84276777dad3c8cfebdf8e739606f90c9, https://git.kernel.org/stable/c/5b14cf37b9f01de0b28c6f8960019d4c7883ce42, https://git.kernel.org/stable/c/b71f4ade1b8900d30c661d6c27f87c35214c398c	O-LIN-LINU-050624/88

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52773**		
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/3a23b384e7e3d64d5587ad10729a34d4f761517e, https://git.kernel.org/stable/c/5b82e4240533bcd4691e50b64ec86d0d7fbd21b9, https://git.kernel.org/stable/c/b028f89c56e964a22d3ddb8eab1a0e7e980841b9	O-LIN-LINU-050624/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in case one is added in future, harden the code by adding the check **CVE ID: CVE-2023-52802**		
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52806**	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42fda2d486f67745d7, https://git.kernel.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	O-LIN-LINU-050624/90
NULL Pointer	21-May-2024	5.5	In the Linux kernel, the	https://git.kernel.org/stable/c	O-LIN-LINU-050624/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			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. **CVE ID: CVE-2023-52809**	/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495ebecbb9395101f3be177cd0a52450b	
NULL Pointer Dereferenc e	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix potential null	https://git.kernel.org/stable/c/80285ae1ec8717b597b20de38866c29d84d321a1, https://git.kernel.org/stable/c/9b70fc7d70e8ef7c4a65034c9	O-LIN-LINU-050624/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer derefernce The amdgpu_ras_get_context may return NULL if device not support ras feature, so add check before using. **CVE ID: CVE-2023-52814**	487f58609e708a1, https://git.kernel.org/stable/c/b0702ee4d811708251cdf54d4a1d3e888d365111	
NULL Pointer Dereference	21-May-2024	5.5	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.	https://git.kernel.org/stable/c/33fb1a555354bd593f785935ddcb5d9dd4d3847f, https://git.kernel.org/stable/c/70f831f21155c692bb336c434936fd6f24f3f81a, https://git.kernel.org/stable/c/8c6c85a073768df68c1a3fea143d013a38c66d34	O-LIN-LINU-050624/93

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-52815		
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: 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	https://git.kernel.org/stable/c/174f62a0aa15c211e60208b41ee9e7cdfb73d455, https://git.kernel.org/stable/c/437e0fa907ba39b4d7eda863c03ea9cf48bd93a9, https://git.kernel.org/stable/c/5104fdf50d326db2c1a994f8b35dcd46e63ae4ad	O-LIN-LINU-050624/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 00000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22 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 ttm edac_mce_amd kvm_amd ccp mac_hid k10temp kvm acpi_ipmi ipmi_si rapl sch_fq_codel ipmi_devintf ipmi_msghandler msr parport_pc ppdev lp parport mtd pstore_blk efi_pstore ramoops		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2023-52817**		
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/panel: fix a possible null	https://git.kernel.org/stable/c/2381f6b628b3214f07375e0adf5ce17093c31190, https://git.kernel.org/stable/c/4fa930ba046d20fc189977039	O-LIN-LINU-050624/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52821**	6ee11e905fa96e4, https://git.kernel.org/stable/c/79813cd59398015867d51e6d7dcc14d287d4c402	
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.28					
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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	https://git.kernel.org/stable/c/10a9d6a7513f93d7faffcb341af0aa42be8218fe, https://git.kernel.org/stable/c/7ac10c7d728d75bc9daaa8fade3c7a3273b9a9ff, https://git.kernel.org/stable/c/c60ed825530b8c0cc2b524efd39b1d696ec54004	O-LIN-LINU-050624/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not be able to free it. Fix it by assigning it properly immediately after allocation. **CVE ID: CVE-2024-35972**		
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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. **CVE ID: CVE-2024-35978**	https://git.kernel.org/stable/c/45d355a926ab40f3ae7bc0b0a00cb0e3e8a5a810, https://git.kernel.org/stable/c/4beab84fbb50df3be1d8f8a976e6fe882ca65cb2, https://git.kernel.org/stable/c/66fab1e120b39f8f47a94186ddee36006fc02ca8	O-LIN-LINU-050624/97
Loop with Unreachable Exit Condition ('Infinite Loop')	20-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: batman-adv: Avoid infinite loop trying to resize local TT	https://git.kernel.org/stable/c/04720ea2e6c64459a90ca28570ea78335eccd924, https://git.kernel.org/stable/c/3fe79b2c83461edbbf86ed8a6f3924820ff892	O-LIN-LINU-050624/98

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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	59, https://git.kernel.org/stable/c/4ca2a5fb54ea2cc43edea614207fcede562d91c2	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. 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.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code is able to handle also the situations when there were already incompatible system configuration are present. **CVE ID: CVE-2024-35982**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.30					
NULL Pointer Dereference	20-May-2024	5.5	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.	https://git.kernel.org/stable/c/357c64ef1ef39b1e7cd91ab6bdd304d043702c83, https://git.kernel.org/stable/c/40f1d79f07b49c8a64a861706e5163f2db4bd95d, https://git.kernel.org/stable/c/4e75e222d397c6752b229ed72fc4644c8c36ecde	O-LIN-LINU-050624/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[wsa: dropped the simplification in core-smbus to avoid theoretical regressions] **CVE ID: CVE-2024-35984**		
Improper Locking	20-May-2024	5.5	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_cha	https://git.kernel.org/stable/c/0ccac964520a6f19e355652c8ca38af2a7f27076, https://git.kernel.org/stable/c/244296cc3a155199a8b080d19e645d7d49081a38, https://git.kernel.org/stable/c/8bf574183282d219cfa991f7df37aad491d74c11	O-LIN-LINU-050624/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n_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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 0000000000000001 [31.079613] x11: 0001ffc083bb2e34 x10: 0001ff880164e98f x9 : 0001ffc082aa3def [31.079824] x8 : 0001ffc082aa3dec x7 : 0000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00 x6 : 0000000000000516 [31.079982] x5 : ffffffc7f8d43000 x4 : ffffff88003c9c40 x3 : ffffffffffffffff [31.080147] x2 : ffffffc7f8d43000 x1 : 0000000000000c0 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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 ID: CVE-2024-35990**		
Out-of-bounds Read	20-May-2024	5.5	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'	https://git.kernel.org/stable/c/40406dfbc060503d2e0a9e637e98493c54997b3d, https://git.kernel.org/stable/c/610f175d2e16fb2436ba7974b990563002c20d07, https://git.kernel.org/stable/c/976df695f579bbb2914114b4e9974fe4ed1eb813	O-LIN-LINU-050624/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2024-35992**		
Improper Locking	20-May-2024	5.5	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. However, this is not necessary, because I2C core already has its own	https://git.kernel.org/stable/c/0561b65fbd53d3e788c5b0222d9112ca016fd6a1, https://git.kernel.org/stable/c/21bfca822cfc1e71796124e93b46e0d9fa584401, https://git.kernel.org/stable/c/29e94f295bad5be59cf4271a93e22cdcf5536722	O-LIN-LINU-050624/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35997**		
NULL Pointer Dereference	20-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/03b5a9b2b526862b21bcc31976e393a6e63785d1,	O-LIN-LINU-050624/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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	https://git.kernel.org/stable/c/58a4c9b1e5a3e53c9148e80b90e1e43897ce77d1, https://git.kernel.org/stable/c/7a25bfd12733a8f38f8ca47c581f876c3d481ac0	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 0000000004001e		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ac RDI: ffff8880160c64c0 RBP: ffffc900015ff060 R08: 0000000000000000 R09: ffff88800f7a4000 R10: 0000000000000002 R11: ffff88800f4f90c0 R12: dfffc0000000000 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: 0000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00 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_sk		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			b_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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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+0x 7c/0x90 kernel/bpf/syscall.c:5199 **CVE ID: CVE-2024-36008**		
Affected Version(s): From (including) 6.3 Up to (excluding) 6.5.13					
Use After Free	21-May-2024	7.8	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	https://git.kernel.org/stable/c/6afc57ea315e0f660b1f870a681737bb7b71faef, https://git.kernel.org/stable/c/afd3425bd69610f318403084fe491e24a1357fb9, https://git.kernel.org/stable/c/d908ca431e20b0e4bfc5d911	O-LIN-LINU-050624/104

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52769**	d1744910ed779bdb	
Affected Version(s): From (including) 6.3 Up to (excluding) 6.6.4					
NULL Pointer Dereference	21-May-2024	5.5	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-	https://git.kernel.org/stable/c/61a55071653974dab172d4c5d699bb365cfd13c9, https://git.kernel.org/stable/c/8ba2c459668cfe2aaacc5ebcd35b4b9ef8643013	O-LIN-LINU-050624/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>mac_table' is allocated. The null pointer will causes the kernel panic. **CVE ID: CVE-2023-52783**		
Affected Version(s): From (including) 6.6 Up to (excluding) 6.6.3					
Use After Free	21-May-2024	7.8	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	https://git.kernel.org/stable/c/0ab6f842452ce2cae04209d4671ac6289d0aef8a, https://git.kernel.org/stable/c/558817597d5fbd7af31f891b67b0fd20f0d047b7, https://git.kernel.org/stable/c/89929ea46f9cc11ba66d2c64713aa5d5dc723b09	O-LIN-LINU-050624/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[816.251274] general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b6d81: 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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 **CVE ID: CVE-2023-52752**		
Use After Free	21-May-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix htt mlo-offset event locking The ath12k active pdevs are	https://git.kernel.org/stable/c/6afc57ea315e0f660b1f870a681737bb7b71faef, https://git.kernel.org/stable/c/afd3425bd69610f318403084fe491e24a1357fb9, https://git.kern	O-LIN-LINU-050624/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52769**	el.org/stable/c/d908ca431e20b0e4bfc5d911d1744910ed779bdb	
Use After Free	21-May-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: af_unix: fix use-after-free in unix_stream_read_actor() syzbot reported the following crash [1]	https://git.kernel.org/stable/c/069a3ec329ff43e7869a3d94c62cd03203016bce, https://git.kernel.org/stable/c/4b7b492615cf3017190f55444f7016812b66611d, https://git.kernel.org/stable/c/75bcfc188abf4fae9c1d5f5dc	O-LIN-LINU-050624/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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,	0a03540be602eef	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fc6748ab228 EFLAGS: 00000246 ORIG_RAX: 00000000000002f RAX: ffffffffffffffda RBX: 0000000000000001c 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			</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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2023-52772**		
Out-of-bounds Read	21-May-2024	7.1	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	https://git.kernel.org/stable/c/1bc44a505a229bb1dd4957e11aa594edeea3690e, https://git.kernel.org/stable/c/79527c21a3ce04cffc35ea54f74ee087e532be57, https://git.kernel.org/stable/c/c9e44111da221246efb2e623	O-LIN-LINU-050624/109

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52827**	ae1be40a5cf6542c	
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid NULL dereference of timing generator [Why & How]	https://git.kernel.org/stable/c/09909f515032fa80b921fd3118efe66b185d10fd, https://git.kernel.org/stable/c/4e497f1acd99075b13605b2e7fa0cba721a2cfd9, https://git.kern	O-LIN-LINU-050624/110

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Check whether assigned timing generator is NULL or not before accessing its funcs to prevent NULL dereference. **CVE ID: CVE-2023-52753**	el.org/stable/c/6d8653b1a7a8dc938b566ae8c4f373b36e792c68	
NULL Pointer Dereference	21-May-2024	5.5	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	https://git.kernel.org/stable/c/1d07b7e84276777dad3c8cfebdf8e739606f90c9, https://git.kernel.org/stable/c/5b14cf37b9f01de0b28c6f8960019d4c7883ce42, https://git.kernel.org/stable/c/b71f4ade1b8900d30c661d6c27f87c35214c398c	O-LIN-LINU-050624/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IGT test) then fail the amdgpu_dm_i2c_xfer() call. **CVE ID: CVE-2023-52773**		
NULL Pointer Dereference	21-May-2024	5.5	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 **CVE ID: CVE-2023-52802**	https://git.kernel.org/stable/c/3a23b384e7e3d64d5587ad10729a34d4f761517e, https://git.kernel.org/stable/c/5b82e4240533bcd4691e50b64ec86d0d7fbd21b9, https://git.kernel.org/stable/c/b028f89c56e964a22d3ddb8eab1a0e7e980841b9	O-LIN-LINU-050624/112
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2527775616f3638f4fd54649eba8c7b84d5e	O-LIN-LINU-050624/113

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52806**	4250, https://git.kernel.org/stable/c/25354bae4fc310c3928e8a42fda2d486f67745d7, https://git.kernel.org/stable/c/43b91df291c8802268ab3cfd8fccfdf135800ed4	
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: scsi: libfc: Fix potential NULL pointer dereference in fc_lport_ptp_setup()	https://git.kernel.org/stable/c/442fd24d7b6b29e4a9cd9225afba4142d5f522ba, https://git.kernel.org/stable/c/4df105f0ce9f6f30cda4e99f577150d23f0c9c5f, https://git.kernel.org/stable/c/56d78b5495e	O-LIN-LINU-050624/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID: CVE-2023-52809**	becbb9395101f3be177cd0a52450b	
NULL Pointer Dereference	21-May-2024	5.5	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.	https://git.kernel.org/stable/c/80285ae1ec8717b597b20de38866c29d84d321a1, https://git.kernel.org/stable/c/9b70fc7d70e8ef7c4a65034c9487f58609e708a1, https://git.kernel.org/stable/c/b0702ee4d811708251cdf54d4a1d3e888d365111	O-LIN-LINU-050624/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-52814		
NULL Pointer Dereference	21-May-2024	5.5	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. **CVE ID: CVE-2023-52815**	https://git.kernel.org/stable/c/33fb1a555354bd593f785935ddcb5d9dd4d3847f, https://git.kernel.org/stable/c/70f831f21155c692bb336c434936fd6f24f3f81a, https://git.kernel.org/stable/c/8c6c85a073768df68c1a3fea143d013a38c66d34	O-LIN-LINU-050624/116
NULL Pointer Dereference	21-May-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix a null pointer access when the	https://git.kernel.org/stable/c/174f62a0aa15c211e60208b41ee9e7cdfb73d455, https://git.kernel.org/stable/c/437e0fa907ba39b4d7eda863c03ea9cf48bd9	O-LIN-LINU-050624/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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:	3a9, https://git.kernel.org/stable/c/5104fdf50d326db2c1a994f8b35dcd46e63ae4ad	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_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 ec 28 48 89 54 24		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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: 00000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			03 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 tm edac_mce_amd kvm_amd ccp mac_hid k10temp kvm acpi_ipmi ipmi_si rapl sch_fq_codel ipmi_devintf ipmi_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)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2023-52817**		
NULL Pointer Dereference	21-May-2024	5.5	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()	https://git.kernel.org/stable/c/2381f6b628b3214f07375e0adf5ce17093c31190, https://git.kernel.org/stable/c/4fa930ba046d20fc1899770396ee11e905fa96e4, https://git.kernel.org/stable/c/79813cd59398015867d51e6d7dcc14d287d4c402	O-LIN-LINU-050624/118

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2023-52821**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.8.7					
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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. **CVE ID: CVE-2024-35972**	https://git.kernel.org/stable/c/10a9d6a7513f93d7faffcb341af0aa42be8218fe, https://git.kernel.org/stable/c/7ac10c7d728d75bc9daaa8fade3c7a3273b9a9ff, https://git.kernel.org/stable/c/c60ed825530b8c0cc2b524efd39b1d696ec54004	O-LIN-LINU-050624/119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	20-May-2024	5.5	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. **CVE ID: CVE-2024-35978**	https://git.kernel.org/stable/c/45d355a926ab40f3ae7bc0b0a00cb0e3e8a5a810, https://git.kernel.org/stable/c/4beab84fbb50df3be1d8f8a976e6fe882ca65cb2, https://git.kernel.org/stable/c/66fab1e120b39f8f47a94186ddee36006fc02ca8	O-LIN-LINU-050624/120
Loop with Unreachable Exit Condition ('Infinite Loop')	20-May-2024	5.5	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	https://git.kernel.org/stable/c/04720ea2e6c64459a90ca28570ea78335eccd924, https://git.kernel.org/stable/c/3fe79b2c83461edbbf86ed8a6f3924820ff89259, https://git.kernel.org/stable/c/4ca2a5fb54ea2cc43edea614207fcede562d91c2	O-LIN-LINU-050624/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			timeout will be halved all the time and will then stagnate at 0 and therefore never be able to reduce the table even more. 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 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.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35982		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.8.9					
NULL Pointer Dereference	20-May-2024	5.5	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] **CVE ID: CVE-2024-35984**	https://git.kernel.org/stable/c/357c64ef1ef39b1e7cd91ab6bdd304d043702c83, https://git.kernel.org/stable/c/40f1d79f07b49c8a64a861706e5163f2db4bd95d, https://git.kernel.org/stable/c/4e75e222d397c6752b229ed72fc4644c8c36ecde	O-LIN-LINU-050624/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	20-May-2024	5.5	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	https://git.kernel.org/stable/c/0ccac964520a6f19e355652c8ca38af2a7f27076, https://git.kernel.org/stable/c/244296cc3a155199a8b080d19e645d7d49081a38, https://git.kernel.org/stable/c/8bf574183282d219cfa991f7df37aad491d74c11	O-LIN-LINU-050624/123

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[31.080147] x2 : ffffffc7f8d43000 x1 : 0000000000000c0 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[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		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[31.084932] irq event stamp: 64549 [31.084970] hardirqs last enabled at (64548): [<ffffffc081adf35c>] _raw_spin_unlock_irqrestore+0x80/0x90 [31.085157] ---truncated--- **CVE ID: CVE-2024-35990**		
Out-of-bounds Read	20-May-2024	5.5	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	https://git.kernel.org/stable/c/40406dfbc060503d2e0a9e637e98493c54997b3d, https://git.kernel.org/stable/c/610f175d2e16fb2436ba7974b990563002c20d07, https://git.kernel.org/stable/c/976df695f579bbb2914114b4e9974fe4ed1eb813	O-LIN-LINU-050624/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			]' is used when all elements of 'gbe_phy_init_fix' array are handled. Found by Linux Verification Center (linuxtesting.org) with SVACE. **CVE ID: CVE-2024-35992**		
Improper Locking	20-May-2024	5.5	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. 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	https://git.kernel.org/stable/c/0561b65fbd53d3e788c5b0222d9112ca016fd6a1, https://git.kernel.org/stable/c/21bfca822cfc1e71796124e93b46e0d9fa584401, https://git.kernel.org/stable/c/29e94f295bad5be59cf4271a93e22cdcf5536722	O-LIN-LINU-050624/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 ID: CVE-2024-35997**		
NULL Pointer Dereference	20-May-2024	5.5	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].	https://git.kernel.org/stable/c/03b5a9b2b526862b21bcc31976e393a6e63785d1, https://git.kernel.org/stable/c/58a4c9b1e5a3e53c9148e80b90e1e43897ce77d1, https://git.kernel.org/stable/c/7a25bfd12733a8f38f8ca47c5	O-LIN-LINU-050624/126

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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	81f876c3d481ac0	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: dfffc0000000000 R13: 0000000000000000 R14: 00000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00 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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 **CVE ID: CVE-2024-36008**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions