National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 – 31 Jul 2024 Vol. 11 No. 14
https://nciipc.gov.in/

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Acronis					
Product: cyber_infrastructure					
Affected Version(s): * Up to (excluding) 5.0.1-61					
Improper Authentication	24-Jul-2024	9.8	Remote command execution due to use of default passwords. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.0.1-61, Acronis Cyber Infrastructure (ACI) before build 5.1.1-71, Acronis Cyber Infrastructure (ACI) before build 5.2.1-69, Acronis Cyber Infrastructure (ACI) before build 5.3.1-53, Acronis Cyber Infrastructure (ACI) before build 5.4.4-132. **CVE ID: CVE-2023-45249**	https://security-advisory.acronis.com/advisories/SEC-6452	A-ACR-CYBE-020824/1
Affected Version(s): From (including) 5.1.1 Up to (excluding) 5.1.1-71					
Improper Authentication	24-Jul-2024	9.8	Remote command execution due to use of default passwords. The following products are affected: Acronis Cyber	https://security-advisory.acronis.com/advisories/SEC-6452	A-ACR-CYBE-020824/2

CVSS 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
			Infrastructure (ACI) before build 5.0.1-61, Acronis Cyber Infrastructure (ACI) before build 5.1.1-71, Acronis Cyber Infrastructure (ACI) before build 5.2.1-69, Acronis Cyber Infrastructure (ACI) before build 5.3.1-53, Acronis Cyber Infrastructure (ACI) before build 5.4.4-132. **CVE ID: CVE-2023-45249**		
Affected Version(s): From (including) 5.2.1 Up to (excluding) 5.2.1-69					
Improper Authentication	24-Jul-2024	9.8	Remote command execution due to use of default passwords. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.0.1-61, Acronis Cyber Infrastructure (ACI) before build 5.1.1-71, Acronis Cyber Infrastructure (ACI) before build 5.2.1-69, Acronis Cyber Infrastructure (ACI) before build	https://security-advisory.acronis.com/advisories/SEC-6452	A-ACR-CYBE-020824/3

CVSS 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
			5.3.1-53, Acronis Cyber Infrastructure (ACI) before build 5.4.4-132. **CVE ID: CVE-2023-45249**		
Affected Version(s): From (including) 5.3.1 Up to (excluding) 5.3.1-53					
Improper Authentication	24-Jul-2024	9.8	Remote command execution due to use of default passwords. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.0.1-61, Acronis Cyber Infrastructure (ACI) before build 5.1.1-71, Acronis Cyber Infrastructure (ACI) before build 5.2.1-69, Acronis Cyber Infrastructure (ACI) before build 5.3.1-53, Acronis Cyber Infrastructure (ACI) before build 5.4.4-132. **CVE ID: CVE-2023-45249**	https://security-advisory.acronis.com/advisories/SEC-6452	A-ACR-CYBE-020824/4
Affected Version(s): From (including) 5.4.4 Up to (excluding) 5.4.4-132					
Improper Authentication	24-Jul-2024	9.8	Remote command execution due to use of default passwords. The following products	https://security-advisory.acronis.com/advisories/SEC-6452	A-ACR-CYBE-020824/5

CVSS 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
			are affected: Acronis Cyber Infrastructure (ACI) before build 5.0.1-61, Acronis Cyber Infrastructure (ACI) before build 5.1.1-71, Acronis Cyber Infrastructure (ACI) before build 5.2.1-69, Acronis Cyber Infrastructure (ACI) before build 5.3.1-53, Acronis Cyber Infrastructure (ACI) before build 5.4.4-132. **CVE ID: CVE-2023-45249**		
Vendor: afthemes					
Product: wp_post_author					
Affected Version(s): * Up to (excluding) 3.6.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AF themes WP Post Author allows Stored XSS.This issue affects WP Post Author: from n/a through 3.6.7. **CVE ID: CVE-2024-37101**	N/A	A-AFT-WP_P-020824/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: aipower					
Product: aipower					
Affected Version(s): * Up to (excluding) 1.8.67					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Senol Sahin GPT3 AI Content Writer allows Stored XSS.This issue affects GPT3 AI Content Writer: from n/a through 1.8.66. **CVE ID: CVE-2024-37465**	N/A	A-AIP-AIPO-020824/7
Vendor: ali2woo					
Product: aliexpress_dropshipping_with_alinext					
Affected Version(s): * Up to (excluding) 3.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ali2Woo Team Ali2Woo Lite allows Reflected XSS.This issue affects Ali2Woo Lite: from n/a through 3.3.5. **CVE ID: CVE-2024-37211**	N/A	A-ALI-ALIE-020824/8
Vendor: Apache					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: airflow					
Affected Version(s): * Up to (excluding) 2.9.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	5.4	Apache Airflow versions before 2.9.3 have a vulnerability that allows an authenticated attacker to inject a malicious link when installing a provider. Users are recommended to upgrade to version 2.9.3, which fixes this issue. **CVE ID: CVE-2024-39863**	https://github.com/apache/airflow/pull/40475	A-APA-AIRF-020824/9
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.9.3					
Improper Control of Generation of Code ('Code Injection')	17-Jul-2024	8.8	Apache Airflow 2.4.0, and versions before 2.9.3, has a vulnerability that allows authenticated DAG authors to craft a doc_md parameter in a way that could execute arbitrary code in the scheduler context, which should be forbidden according to the Airflow Security model. Users should upgrade to version 2.9.3 or later which has removed the vulnerability.	https://github.com/apache/airflow/pull/40522	A-APA-AIRF-020824/10

CVSS 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-2024-39877		
Product: cxf					
Affected Version(s): * Up to (excluding) 3.5.9					
N/A	19-Jul-2024	7.5	An improper input validation of the p2c parameter in the Apache CXF JOSE code before 4.0.5, 3.6.4 and 3.5.9 allows an attacker to perform a denial of service attack by specifying a large value for this parameter in a token. **CVE ID: CVE-2024-32007**	https://lists.apache.org/thread/stwrgsr1llb73nkl16klv9vjqgmmx633	A-APA-CXF-020824/11
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.4					
N/A	19-Jul-2024	7.5	An improper input validation of the p2c parameter in the Apache CXF JOSE code before 4.0.5, 3.6.4 and 3.5.9 allows an attacker to perform a denial of service attack by specifying a large value for this parameter in a token. **CVE ID: CVE-2024-32007**	https://lists.apache.org/thread/stwrgsr1llb73nkl16klv9vjqgmmx633	A-APA-CXF-020824/12
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.5					
N/A	19-Jul-2024	7.5	An improper input validation of	https://lists.apache.org/thread/	A-APA-CXF-020824/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the p2c parameter in the Apache CXF JOSE code before 4.0.5, 3.6.4 and 3.5.9 allows an attacker to perform a denial of service attack by specifying a large value for this parameter in a token. **CVE ID: CVE-2024-32007**	stwrgsr1llb73nkl16klv9vjqgmmx633	
Product: streampark					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Jul-2024	4.7	In streampark, the project module integrates Maven's compilation capabilities. The input parameter validation is not strict, allowing attackers to insert commands for remote command execution, The prerequisite for a successful attack is that the user needs to log in to the streampark system and have system-level permissions. Generally, only users of that system have the authorization to log in, and users would not manually input a dangerous	N/A	A-APA-STRE-020824/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation command. Therefore, the risk level of this vulnerability is very low. Background: In the "Project" module, the maven build args “<” operator causes command injection. e.g : “< (curl http://xxx.com)” will be executed as a command injection, Mitigation: all users should upgrade to 2.1.4, The "<" operator will blocked。 **CVE ID: CVE-2023-52291**		
Improper Neutralization of Special Elements used in a Command ('Comman	17-Jul-2024	4.7	In streampark, the project module integrates Maven's compilation capabilities. The input parameter validation is not strict, allowing attackers to insert	N/A	A-APA-STRE-020824/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			commands for remote command execution, The prerequisite for a successful attack is that the user needs to log in to the streampark system and have system-level permissions. Generally, only users of that system have the authorization to log in, and users would not manually input a dangerous operation command. Therefore, the risk level of this vulnerability is very low. Mitigation: all users should upgrade to 2.1.4 Background info: Log in to Streampark using the default username (e.g. test1, test2, test3) and the default password (streampark). Navigate to the Project module,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then add a new project. Enter the git repository address of the project and input `touch /tmp/success_2.1.2 ` as the "Build Argument". Note that there is no verification and interception of the special character "`". As a result, you will find that this injection command will be successfully executed after executing the build.  In the latest version, the special symbol ` is intercepted. **CVE ID: CVE-2024-29737**		
Product: streampipes					
Affected Version(s): * Up to (excluding) 0.95.0					
Server-Side Request Forgery (SSRF)	17-Jul-2024	4.3	Server-Side Request Forgery (SSRF) vulnerability in Apache StreamPipes during installation process of pipeline elements. Previously, StreamPipes	https://lists.apache.org/thread/8lryp3bxnby9kmk13odkz2jbfdjfvf0y	A-APA-STRE-020824/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed users to configure custom endpoints from which to install additional pipeline elements. These endpoints were not properly validated, allowing an attacker to get StreamPipes to send an HTTP GET request to an arbitrary address. This issue affects Apache StreamPipes: through 0.93.0. Users are recommended to upgrade to version 0.95.0, which fixes the issue. **CVE ID: CVE-2024-31979**		
Time-of-check Time-of-use (TOCTOU) Race Condition	17-Jul-2024	3.7	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Apache StreamPipes in user self-registration. This allows an attacker to potentially request the creation of	https://lists.apache.org/thread/8yodrmohgcybq900or3d4hc1msl230fr	A-APA-STRE-020824/17

CVSS 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
			multiple accounts with the same email address until the email address is registered, creating many identical users and corrupting StreamPipe's user management. This issue affects Apache StreamPipes: through 0.93.0. Users are recommended to upgrade to version 0.95.0, which fixes the issue. **CVE ID: CVE-2024-30471**		
Vendor: apollo13themes					
Product: apollo13_framework_extensions					
Affected Version(s): * Up to (excluding) 1.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Apollo13Themes Apollo13 Framework Extensions apollo13-framework-extensions allows	N/A	A-APO-APOL-020824/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored XSS.This issue affects Apollo13 Framework Extensions: from n/a through 1.9.3. **CVE ID: CVE-2024-37480**		
Vendor: archerirm					
Product: archer					
Affected Version(s): * Up to (excluding) 2024.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2024	5.4	An issue was discovered in Archer Platform 6 before 2024.06. Authenticated users can achieve HTML content injection. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. **CVE ID: CVE-2024-41707**	https://www.archerirm.community/t5/platform-announcements/archer-update-for-multiple-vulnerabilities/ta-p/739717	A-ARC-ARCH-020824/19
Affected Version(s): * Up to (excluding) 6.13.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2024	5.4	A stored XSS issue was discovered in Archer Platform 6.8 before 2024.06. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. 6.14.P4 (6.14.0.4) and 6.13 P4 (6.13.0.4) are also fixed releases. This vulnerability is similar to, but not identical to, CVE-2023-30639. **CVE ID: CVE-2024-41705**	https://www.archerirm.community/t5/platform-announcements/archer-update-for-multiple-vulnerabilities/ta-p/739717	A-ARC-ARCH-020824/20
Affected Version(s): * Up to (excluding) 6.14.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2024	5.4	A stored XSS issue was discovered in Archer Platform 6 before version 2024.06. A remote authenticated malicious Archer user could potentially exploit	https://www.archerirm.community/t5/platform-announcements/archer-update-for-multiple-vulnerabilities/ta-p/739717	A-ARC-ARCH-020824/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. 6.14 P4 (6.14.0.4) is also a fixed release. **CVE ID: CVE-2024-41706**		
Affected Version(s): From (including) 2024.03 Up to (excluding) 2024.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2024	5.4	A stored XSS issue was discovered in Archer Platform 6.8 before 2024.06. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable	https://www.archerirm.community/t5/platform-announcements/archer-update-for-multiple-vulnerabilities/ta-p/739717	A-ARC-ARCH-020824/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application. 6.14.P4 (6.14.0.4) and 6.13 P4 (6.13.0.4) are also fixed releases. This vulnerability is similar to, but not identical to, CVE-2023-30639. **CVE ID: CVE-2024-41705**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2024	5.4	A stored XSS issue was discovered in Archer Platform 6 before version 2024.06. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. 6.14 P4 (6.14.0.4) is also a fixed release. **CVE ID: CVE-2024-41706**	https://www.archerirm.community/t5/platform-announcements/archer-update-for-multiple-vulnerabilities/ta-p/739717	A-ARC-ARCH-020824/23
Affected Version(s): From (including) 6.14.0 Up to (excluding) 6.14.0.4					
Improper Neutralization of Input	25-Jul-2024	5.4	A stored XSS issue was discovered in Archer Platform 6.8	https://www.archerirm.community/t5/platfor	A-ARC-ARCH-020824/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			before 2024.06. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. 6.14.P4 (6.14.0.4) and 6.13 P4 (6.13.0.4) are also fixed releases. This vulnerability is similar to, but not identical to, CVE-2023-30639. **CVE ID: CVE-2024-41705**	m-announcements/archer-update-for-multiple-vulnerabilities/ta-p/739717	
Vendor: Artistscope					
Product: copysafe_web_protection					
Affected Version(s): * Up to (excluding) 4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ArtistScope CopySafe Web	N/A	A-ART-COPY-020824/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protection allows Reflected XSS.This issue affects CopySafe Web Protection: from n/a through 3.15. **CVE ID: CVE-2024-38781**		
Vendor: Arubanetworks					
Product: edgeconnect_sd-wan_orchestrator					
Affected Version(s): 8.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-2024	8.8	An authenticated command injection vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateways Command Line Interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID: CVE-2024-41136**	https://csaf.arubanetworks.com/2024/hpe_aruba_networking_-_hpesbnw04673.txt	A-ARU-EDGE-020824/26
Affected Version(s): 9.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Jul-2024	8.8	An authenticated command injection vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateways Command Line Interface.	https://csaf.arubanetworks.com/2024/hpe_aruba_networking_-_hpesbnw04673.txt	A-ARU-EDGE-020824/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID: CVE-2024-41136**		
Affected Version(s): 9.3.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-2024	8.8	An authenticated command injection vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateways Command Line Interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID: CVE-2024-41136**	https://csaf.arubanetworks.com/2024/hpe_aruba_networking_-_hpesbnw04673.txt	A-ARU-EDGE-020824/28
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.10					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	24-Jul-2024	8.8	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conduct a server-side prototype pollution attack. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-22443**		
Affected Version(s): From (including) 9.1.0 Up to (including) 9.1.11					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-2024	8.8	An authenticated command injection vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateways Command Line Interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID: CVE-2024-41136**	https://csaf.arubanetworks.com/2024/hpe_aruba_networking_-_hpesbnw04673.txt	A-ARU-EDGE-020824/30
Affected Version(s): From (including) 9.1.0 Up to (including) 9.1.9					
Improper Neutralization of Input During	24-Jul-2024	9	A vulnerability in the web-based management interface of	https://support.hpe.com/hpesc/public/docDisplay?docId=hpe	A-ARU-EDGE-020824/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID: CVE-2024-41914**	sbnw04672en_us&docLocale=en_US	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	6.1	A vulnerability within the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victims browser in the context of the affected interface. **CVE ID: CVE-2024-22444**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.10					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	24-Jul-2024	8.8	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a server-side prototype pollution attack. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-22443**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/33
Affected Version(s): From (including) 9.2.0 Up to (including) 9.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	9	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/34

CVSS 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
			allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID: CVE-2024-41914**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-2024	8.8	An authenticated command injection vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateways Command Line Interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID: CVE-2024-41136**	https://csaf.arubanetworks.com/2024/hpe_aruba_networking_-_hpesbnw04673.txt	A-ARU-EDGE-020824/35
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	6.1	A vulnerability within the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/36

CVSS 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
			attacker to execute arbitrary script code in a victims browser in the context of the affected interface. **CVE ID: CVE-2024-22444**		
Affected Version(s): From (including) 9.3.0 Up to (excluding) 9.3.3					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	24-Jul-2024	8.8	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a server-side prototype pollution attack. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-22443**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/37
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	6.1	A vulnerability within the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow a remote attacker to	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victims browser in the context of the affected interface. **CVE ID: CVE-2024-22444**		
Affected Version(s): From (including) 9.3.0 Up to (including) 9.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	9	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID: CVE-2024-41914**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/39
Affected Version(s): From (including) 9.4.0 Up to (excluding) 9.4.2					

CVSS 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
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	24-Jul-2024	8.8	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a server-side prototype pollution attack. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise. **CVE ID: CVE-2024-22443**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/40
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	6.1	A vulnerability within the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victims	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser in the context of the affected interface. **CVE ID: CVE-2024-22444**		
Affected Version(s): From (including) 9.4.0 Up to (including) 9.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	9	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID: CVE-2024-41914**	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US	A-ARU-EDGE-020824/42
Vendor: atarim					
Product: atarim					
Affected Version(s): * Up to (excluding) 3.32					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Atarim allows	N/A	A-ATA-ATAR-020824/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored XSS.This issue affects Atarim: from n/a through 3.31. **CVE ID: CVE-2024-37434**		
Vendor: auburnforest					
Product: blogmentor					
Affected Version(s): * Up to (including) 1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AuburnForest Blogmentor – Blog Layouts for Elementor allows Stored XSS.This issue affects Blogmentor – Blog Layouts for Elementor: from n/a through 1.5. **CVE ID: CVE-2024-37229**	N/A	A-AUB-BLOG-020824/44
Vendor: backdropcms					
Product: backdrop					
Affected Version(s): From (including) 1.27.0 Up to (excluding) 1.27.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Backdrop CMS before 1.27.3 and 1.28.x before 1.28.2 does not sufficiently sanitize field labels before they are displayed in certain places. This vulnerability is	https://backdropcms.org/security/backdrop-sa-core-2024-001	A-BAC-BACK-020824/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mitigated by the fact that an attacker must have a role with the "administer fields" permission. **CVE ID: CVE-2024-41709**		
Affected Version(s): From (including) 1.28.0 Up to (excluding) 1.28.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Backdrop CMS before 1.27.3 and 1.28.x before 1.28.2 does not sufficiently sanitize field labels before they are displayed in certain places. This vulnerability is mitigated by the fact that an attacker must have a role with the "administer fields" permission. **CVE ID: CVE-2024-41709**	https://backdropcms.org/security/backdrop-sa-core-2024-001	A-BAC-BACK-020824/46
Vendor: bplugins					
Product: html5_audio_player					
Affected Version(s): * Up to (excluding) 2.2.24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bPlugins Html5 Audio Player allows Stored XSS.This issue affects Html5	N/A	A-BPL-HTML-020824/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Audio Player: from n/a through 2.2.23. **CVE ID: CVE-2024-37445**		
Vendor: brainstormforce					
Product: cards_for_beaver_builder					
Affected Version(s): * Up to (excluding) 1.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pratik Chaskar Cards for Beaver Builder.This issue affects Cards for Beaver Builder: from n/a through 1.1.4. **CVE ID: CVE-2024-37278**	N/A	A-BRA-CARD-020824/48
Product: elementor_-_header\,_footer_\&_blocks_template					
Affected Version(s): * Up to (excluding) 1.6.36					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force, Nikhil Chavan Elementor – Header, Footer & Blocks Template allows DOM-Based XSS.This issue affects Elementor – Header, Footer &	N/A	A-BRA-ELEM-020824/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Blocks Template: from n/a through 1.6.35. **CVE ID: CVE-2024-33933**		
Product: ultimate_addons_for_wpbakery_page_builder					
Affected Version(s): * Up to (excluding) 3.19.20.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	5.4	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_pricing shortcode in all versions up to, and including, 3.19.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5251**	N/A	A-BRA-ULTI-020824/50
Improper Neutralization of Input During	17-Jul-2024	5.4	The Ultimate Addons for WPBakery plugin for WordPress is	N/A	A-BRA-ULTI-020824/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_info_table shortcode in all versions up to, and including, 3.19.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5252**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	5.4	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ult_team shortcode in all versions up to, and including, 3.19.20 due to insufficient input sanitization and output escaping on user supplied attributes.	N/A	A-BRA-ULTI-020824/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5253**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	5.4	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_info_banner shortcode in all versions up to, and including, 3.19.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	N/A	A-BRA-ULTI-020824/53

CVSS 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-2024-5254		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	5.4	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_dual_color shortcode in all versions up to, and including, 3.19.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5255**	N/A	A-BRA-ULTI-020824/54
Vendor: brizy					
Product: brizy-page_builder					
Affected Version(s): * Up to (excluding) 2.4.45					
Unrestricted Upload of File with Dangerous Type	18-Jul-2024	8.8	The Brizy – Page Builder plugin for WordPress is vulnerable to arbitrary file uploads due to	https://plugins.trac.wordpress.org/browser/brizy/trunk/editor/zip/archiver.php#L264,	A-BRI-BRIZ-020824/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing file extension validation in the validateImageContent function called via storeImages in all versions up to, and including, 2.4.43. This makes it possible for authenticated attackers, with contributor access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. Version 2.4.44 prevents the upload of files ending in .sh and .php. Version 2.4.45 fully patches the issue. **CVE ID: CVE-2024-3242**	https://plugins.trac.wordpress.org/browser/brizy/trunk/editor/zip/archiver.php#L547	
Vendor: burgersoftwares					
Product: cozipress					
Affected Version(s): * Up to (including) 1.0.30					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BurgerThemes CoziPress allows Stored XSS.This issue affects	N/A	A-BUR-COZI-020824/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CoziPress: from n/a through 1.0.30. **CVE ID: CVE-2024-38786**		
Vendor: campcodes					
Product: supplier_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jul-2024	9.8	CampCodes Supplier Management System v1.0 is vulnerable to SQL injection via Supply_Management_System/admin/view_order_items.php?id= . **CVE ID: CVE-2024-41551**	N/A	A-CAM-SUPP-020824/57
Vendor: clinics_patient_management_system_project					
Product: clinics_patient_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jul-2024	7.5	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /print_patients_visits.php. The manipulation of the argument from/to leads to sql injection. The attack can be	N/A	A-CLI-CLIN-020824/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272122 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-6968**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jul-2024	7.5	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /ajax/get_patient_history.php. The manipulation of the argument patient_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272123. **CVE ID: CVE-2024-6969**	N/A	A-CLI-CLIN-020824/59
Vendor: Cminds					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cm_popup					
Affected Version(s): * Up to (excluding) 1.6.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	The CM Popup Plugin for WordPress WordPress plugin before 1.6.6 does not sanitise and escape some of the campaign settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks **CVE ID: CVE-2024-5004**	N/A	A-CMI-CM_P-020824/60
Vendor: code-projects					
Product: simple_task_list					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2024	9.8	A vulnerability was found in itsourcecode Simple Task List 1.0. It has been classified as critical. This affects the function insertUserRecord of the file signUp.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be	N/A	A-COD-SIMP-020824/61

CVSS 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
			used. The associated identifier of this vulnerability is VDB-271707. **CVE ID: CVE-2024-6808**		
Vendor: community_events_project					
Product: community_events					
Affected Version(s): * Up to (excluding) 1.5					
Cross-Site Request Forgery (CSRF)	22-Jul-2024	5.4	The Community Events WordPress plugin before 1.5 does not have CSRF check in place when deleting events, which could allow attackers to make a logged in admin delete arbitrary events via a CSRF attack **CVE ID: CVE-2024-6271**	N/A	A-COM-COMM-020824/62
Vendor: computer_laboratory_management_system_project					
Product: computer_laboratory_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2024	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Computer Laboratory Management System 1.0. Affected is an unknown function of the file /lms/classes/Mast	N/A	A-COM-COMP-020824/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			er.php?f=save_record. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271704. **CVE ID: CVE-2024-6802**		
Vendor: creativeinteractivemedia					
Product: transition_slider					
Affected Version(s): * Up to (including) 2.20.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in creativeinteractive media Transition Slider – Responsive Image Slider and Gallery allows Stored XSS.This issue affects Transition Slider – Responsive Image Slider and Gallery: from n/a through 2.20.3. **CVE ID: CVE-2024-37215**	N/A	A-CRE-TRAN-020824/64
Vendor: depicter					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: depicter					
Affected Version(s): * Up to (excluding) 3.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Depicter Slider and Popup by Averta Depicter Slider allows Stored XSS.This issue affects Depicter Slider: from n/a through 3.0.2. **CVE ID: CVE-2024-37414**	N/A	A-DEP-DEPI-020824/65
Vendor: document_management_system_project					
Product: document_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2024	9.8	A vulnerability has been found in itsourcecode Document Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file insert.php. The manipulation of the argument anothercont leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to	N/A	A-DOC-DOCU-020824/66

CVSS 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 public and may be used. The identifier VDB-271705 was assigned to this vulnerability. **CVE ID: CVE-2024-6803**		
Vendor: dotcamp					
Product: ultimate_blocks					
Affected Version(s): * Up to (excluding) 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ultimate Blocks Ultimate Blocks – Gutenberg Blocks Plugin allows Stored XSS.This issue affects Ultimate Blocks – Gutenberg Blocks Plugin: from n/a through 3.1.9. **CVE ID: CVE-2024-37457**	N/A	A-DOT-ULTI-020824/67
Vendor: elementor					
Product: elementor_pro					
Affected Version(s): * Up to (excluding) 3.21.3					
Improper Neutralization of Input During Web Page Generation	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in	N/A	A-ELE-ELEM-020824/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Elementor Elementor Pro allows Reflected XSS.This issue affects Elementor Pro: from n/a through 3.21.2. **CVE ID: CVE-2024-35656**		
Vendor: emiliaprojects					
Product: progress_planner					
Affected Version(s): * Up to (excluding) 0.9.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Emilia Projects Progress Planner allows Stored XSS.This issue affects Progress Planner: from n/a through 0.9.2. **CVE ID: CVE-2024-37422**	N/A	A-EMI-PROG-020824/69
Vendor: employee_and_visitor_gate_pass_logging_system_project					
Product: employee_and_visitor_gate_pass_logging_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	22-Jul-2024	7.5	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been classified as critical.	N/A	A-EMP-EMPL-020824/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			This affects an unknown part of the file /employee_gatepass/admin/?page=employee/manage_employee. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272121 was assigned to this vulnerability. **CVE ID: CVE-2024-6967**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jul-2024	7.5	A vulnerability, which was classified as critical, has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects some unknown processing of the file /employee_gatepass/classes/Master.php?f=delete_department. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely.	N/A	A-EMP-EMPL-020824/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272351. **CVE ID: CVE-2024-7069**		
Vendor: Foliovision					
Product: fv_flowplayer_video_player					
Affected Version(s): * Up to (excluding) 7.5.47.7212					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	The FV Flowplayer Video Player plugin for WordPress is vulnerable to time-based SQL Injection via the 'exclude' parameter in all versions up to, and including, 7.5.46.7212 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract	https://plugins.trac.wordpress.org/browser/fv-wordpress-flowplayer/trunk/models/video-encoder/class.fv-player-encoder-list-table.php#L308, https://plugins.trac.wordpress.org/changeset/3121532/	A-FOL-FV_F-020824/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information from the database. **CVE ID: CVE-2024-6338**		
Vendor: formlift					
Product: formlift_for_infusionsoft_web_forms					
Affected Version(s): * Up to (excluding) 7.5.18					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jul-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Adrian Tobey FormLift for Infusionsoft Web Forms allows Blind SQL Injection.This issue affects FormLift for Infusionsoft Web Forms: from n/a through 7.5.17. **CVE ID: CVE-2024-38773**	N/A	A-FOR-FORM-020824/73
Vendor: funnelkit					
Product: funnel_builder					
Affected Version(s): * Up to (excluding) 3.4.7					
Missing Authorization	24-Jul-2024	4.3	The Funnel Builder for WordPress by FunnelKit – Customize WooCommerce Checkout Pages, Create Sales Funnels, Order Bumps & One Click Upsells plugin for	https://plugins.trac.wordpress.org/browser/funnel-builder/trunk/modules/checkouts/includes/class-wfacp-ajax-controller.php, https://plugins.	A-FUN-FUNN-020824/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress is vulnerable to unauthorized modification of data due to a missing capability check on multiple functions in all versions up to, and including, 3.4.6. This makes it possible for authenticated attackers, with Contributor-level access and above, to update multiple settings, including templates, designs, checkouts, and other plugin settings. **CVE ID: CVE-2024-6836**	trac.wordpress.org/changeset/3123202/	
Vendor: gallery_slideshow_project					
Product: gallery_slideshow					
Affected Version(s): * Up to (including) 1.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jethin Gallery Slideshow allows Stored XSS.This issue affects Gallery Slideshow: from n/a through 1.4.1. **CVE ID: CVE-2024-37246**	N/A	A-GAL-GALL-020824/75

CVSS 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
Vendor: generatewp					
Product: sketchfab_embed					
Affected Version(s): * Up to (including) 1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rami Yushuvaev Sketchfab Embed allows Stored XSS.This issue affects Sketchfab Embed: from n/a through 1.5. **CVE ID: CVE-2024-37216**	N/A	A-GEN-SKET-020824/76
Vendor: getdbt					
Product: dbt_core					
Affected Version(s): * Up to (excluding) 1.6.14					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2024	7.8	dbt enables data analysts and engineers to transform their data using the same practices that software engineers use to build applications. When a user installs a package in dbt, it has the ability to override macros, materializations, and other core components of dbt. This is by design, as it allows packages to extend and	https://docs.getdbt.com/reference/global-configs/legacy-behaviors#behavior-change-flags, https://github.com/dbt-labs/dbt-core/commit/3c82a0296d227cb1be295356df314c11716f4ff6, https://github.com/dbt-labs/dbt-core/security/advisories/GHSA	A-GET-DBT_-020824/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			customize dbt's functionality. However, this also means that a malicious package could potentially override these components with harmful code. This issue has been fixed in versions 1.8.0, 1.6.14 and 1.7.14. Users are advised to upgrade. There are no kn own workarounds for this vulnerability. Users updating to either 1.6.14 or 1.7.14 will need to set `flags.require_explicit_package_overrides_for_builtin_materializations: False` in their configuration in `dbt_project.yml`. **CVE ID: CVE-2024-40637**	-p3f3-5ccg-83xq	
Affected Version(s): From (including) 1.7.0 Up to (excluding) 1.7.14					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2024	7.8	dbt enables data analysts and engineers to transform their data using the same practices that software engineers use to build applications. When a user installs a package in dbt, it has the ability to	https://docs.getdbt.com/reference/global-configs/legacy-behaviors#behavior-change-flags, https://github.com/dbt-labs/dbt-core/commit/3c82a0296d227c	A-GET-DBT_-020824/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			override macros, materializations, and other core components of dbt. This is by design, as it allows packages to extend and customize dbt's functionality. However, this also means that a malicious package could potentially override these components with harmful code. This issue has been fixed in versions 1.8.0, 1.6.14 and 1.7.14. Users are advised to upgrade. There are no kn own workarounds for this vulnerability. Users updating to either 1.6.14 or 1.7.14 will need to set `flags.require_explicit_package_overrides_for_builtin_materializations: False` in their configuration in `dbt_project.yml`. **CVE ID: CVE-2024-40637**	b1be295356df314c11716f4ff6, https://github.com/dbt-labs/dbt-core/security/advisories/GHSA-p3f3-5ccg-83xq	
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): From (including) 11.8.0 Up to (excluding) 16.11.6					
Unrestricted Upload of	17-Jul-2024	5.3	An issue was discovered in	N/A	A-GIT-GITL-020824/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			GitLab CE/EE affecting all versions starting from 11.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 where it was possible to upload an NPM package with conflicting package data. **CVE ID: CVE-2024-6595**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.0.4					
Unrestricted Upload of File with Dangerous Type	17-Jul-2024	5.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 11.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 where it was possible to upload an NPM package with conflicting package data. **CVE ID: CVE-2024-6595**	N/A	A-GIT-GITL-020824/80
Affected Version(s): From (including) 17.1.0 Up to (excluding) 17.1.2					
Unrestricted Upload of File with Dangerous Type	17-Jul-2024	5.3	An issue was discovered in GitLab CE/EE affecting all versions starting from 11.8 prior to 16.11.6, starting from 17.0 prior to	N/A	A-GIT-GITL-020824/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.4, and starting from 17.1 prior to 17.1.2 where it was possible to upload an NPM package with conflicting package data. **CVE ID: CVE-2024-6595**		
Vendor: givewp					
Product: givewp					
Affected Version(s): * Up to (excluding) 3.14.0					
Authorization Bypass Through User-Controlled Key	19-Jul-2024	5.4	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.13.0 via the 'handleRequest' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with GiveWP Worker-level access and above, to delete and update arbitrary posts. **CVE ID: CVE-2024-5977**	https://plugins.trac.wordpress.org/browser/give/trunk/src/DonationForms/V2/Endpoints/FormActions.php#L96, https://plugins.trac.wordpress.org/changeset/3120745/	A-GIV-GIVE-020824/82
Vendor: Google					
Product: chrome					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 117.0.5938.62					
Out-of-bounds Write	16-Jul-2024	8.8	Out of bounds write in SwiftShader in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-3176**	N/A	A-GOO-CHRO-020824/83
Affected Version(s): * Up to (excluding) 119.0.6045.105					
N/A	16-Jul-2024	8.8	Inappropriate implementation in V8 in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-3174**	N/A	A-GOO-CHRO-020824/84
Affected Version(s): * Up to (excluding) 120.0.6099.62					
Insufficient Verification of Data Authenticity	16-Jul-2024	8.8	Insufficient data validation in Updater in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to perform OS-level privilege escalation via a	https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop.html	A-GOO-CHRO-020824/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious file. (Chromium security severity: High) **CVE ID: CVE-2024-3173**		
N/A	16-Jul-2024	6.3	Insufficient data validation in Extensions in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Low) **CVE ID: CVE-2024-3175**	N/A	A-GOO-CHRO-020824/86
Affected Version(s): * Up to (excluding) 121.0.6167.139					
Use After Free	16-Jul-2024	8.8	Use after free in V8 in Google Chrome prior to 121.0.6167.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-3169**	N/A	A-GOO-CHRO-020824/87
Out-of-bounds Read	16-Jul-2024	6.5	Out of bounds read in V8 in Google Chrome prior to 121.0.6167.139 allowed a remote	https://chromereleases.googleblog.com/2024/01/stable-channel-update-	A-GOO-CHRO-020824/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-2884**	for-desktop_30.html	
Affected Version(s): * Up to (excluding) 121.0.6167.85					
Use After Free	16-Jul-2024	8.8	Use after free in WebRTC in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-3170**	N/A	A-GOO-CHRO-020824/89
N/A	16-Jul-2024	8.8	Insufficient data validation in DevTools in Google Chrome prior to 121.0.6167.85 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-020824/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-3172		
Affected Version(s): * Up to (excluding) 122.0.6261.57					
Use After Free	16-Jul-2024	8.8	Use after free in DevTools in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-3168**	https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-020824/91
Use After Free	16-Jul-2024	8.8	Use after free in Accessibility in Google Chrome prior to 122.0.6261.57 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium) **CVE ID: CVE-2024-3171**	https://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-020824/92
N/A	16-Jul-2024	6.5	Inappropriate implementation in Sign-In in Google Chrome prior to 1.3.36.351 allowed a remote attacker to bypass	N/A	A-GOO-CHRO-020824/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-5500**		
Vendor: groundhogg					
Product: groundhogg					
Affected Version(s): * Up to (excluding) 3.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Groundhogg Inc. Groundhogg allows Reflected XSS.This issue affects Groundhogg: from n/a through 3.4.2.3. **CVE ID: CVE-2024-37264**	N/A	A-GRO-GROU-020824/94
Vendor: holoborodko					
Product: wp_quicklatex					
Affected Version(s): * Up to (excluding) 3.8.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	The WP QuickLaTeX WordPress plugin before 3.8.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored	N/A	A-HOL-WP_Q-020824/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2024-5529**		
Vendor: Huawei					
Product: opengauss					
Affected Version(s): 7.3.0					
N/A	24-Jul-2024	5.5	An issue in Huawei Technologies opengauss (openGauss 5.0.0 build) v.7.3.0 allows a local attacker to cause a denial of service via the modification of table attributes **CVE ID: CVE-2024-40575**	N/A	A-HUA-OPEN-020824/96
Vendor: ibericode					
Product: html_forms					
Affected Version(s): * Up to (excluding) 1.3.33					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	The HTML Forms WordPress plugin before 1.3.33 does not sanitize and escape the form message inputs, allowing high-privilege users, such as administrators, to perform Stored Cross-Site Scripting (XSS) attacks even	N/A	A-IBE-HTML-020824/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when the unfiltered_html capability is disabled. **CVE ID: CVE-2024-6243**		
Vendor: icegram					
Product: email_subscribers_\&_newsletters					
Affected Version(s): * Up to (excluding) 5.7.27					
Missing Authorization	17-Jul-2024	4.3	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to unauthorized API access due to a missing capability check in all versions up to, and including, 5.7.26. This makes it possible for authenticated attackers, with Subscriber-level access and above, to access the API (provided it is enabled) and add, edit, and delete audience users. **CVE ID: CVE-2024-5703**	https://plugins.trac.wordpress.org/changeset/3118326/email-subscribers/trunk/lite/admin/class-es-rest-api-admin.php	A-ICE-EMAI-020824/98
Vendor: idehweb					
Product: login_with_phone_number					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.7.36					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hamid Alinia – idehweb Login with phone number allows Stored XSS.This issue affects Login with phone number: from n/a through 1.7.35. **CVE ID: CVE-2024-37429**	N/A	A-IDE-LOGI-020824/99
Vendor: insurance_management_system_project					
Product: insurance_management_system					
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Jul-2024	7.5	A vulnerability was found in SourceCodester Insurance Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /E-Insurance/. The manipulation leads to direct request. The attack can be launched remotely. The exploit has been disclosed to the	N/A	A-INS-INSU-020824/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The identifier VDB-272365 was assigned to this vulnerability. **CVE ID: CVE-2024-7080**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	4.6	A vulnerability classified as problematic has been found in SourceCodester Insurance Management System 1.0. This affects an unknown part of the file /Script/admin/core/update_sub_category. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272349 was assigned to this vulnerability. **CVE ID: CVE-2024-7068**	N/A	A-INS-INSU-020824/101
Vendor: jegstudio					
Product: gutenverse					
Affected Version(s): * Up to (excluding) 1.9.3					
Improper Neutralization of Input	21-Jul-2024	5.4	Improper Neutralization of Input During Web	N/A	A-JEG-GUTE-020824/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jegstudio Gutenverse allows Stored XSS.This issue affects Gutenverse: from n/a through 1.9.2. **CVE ID: CVE-2024-38785**		
Vendor: jkev					
Product: record_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	A vulnerability was found in SourceCodester Record Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file edit_emp.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271925 was assigned to this vulnerability.	N/A	A-JKE-RECO-020824/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6900		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	A vulnerability classified as critical has been found in SourceCodester Record Management System 1.0. Affected is an unknown function of the file entry.php. The manipulation of the argument school leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-271926 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-6901**	N/A	A-JKE-RECO-020824/104
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	A vulnerability classified as critical was found in SourceCodester Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the file sort_user.php. The manipulation of the argument	N/A	A-JKE-RECO-020824/105

CVSS 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
			sort leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-271927. **CVE ID: CVE-2024-6902**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Record Management System 1.0. Affected by this issue is some unknown functionality of the file sort1_user.php. The manipulation of the argument position leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271928. **CVE ID: CVE-2024-6903**	N/A	A-JKE-RECO-020824/106

CVSS 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 Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Record Management System 1.0. This affects an unknown part of the file sort2_user.php. The manipulation of the argument qualification leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271929 was assigned to this vulnerability. **CVE ID: CVE-2024-6904**	N/A	A-JKE-RECO-020824/107
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	A vulnerability has been found in SourceCodester Record Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_info_user.php . The manipulation of the argument id leads to sql injection. The attack can be	N/A	A-JKE-RECO-020824/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. VDB-271930 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-6905**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	8.8	A vulnerability was found in SourceCodester Record Management System 1.0 and classified as critical. This issue affects some unknown processing of the file add_leave_non_user.php. The manipulation of the argument LSS leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-271931. **CVE ID: CVE-2024-6906**	N/A	A-JKE-RECO-020824/109
Improper Neutralization of Input During	19-Jul-2024	5.4	A vulnerability was found in SourceCodester Record	N/A	A-JKE-RECO-020824/110

CVSS 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
Web Page Generation ('Cross-site Scripting')			Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file sort.php. The manipulation of the argument sort leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271932. **CVE ID: CVE-2024-6907**		
Vendor: kaptinlin					
Product: striking					
Affected Version(s): * Up to (excluding) 2.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in kaptinlin Striking allows Reflected XSS.This issue affects Striking: from n/a through 2.3.4. **CVE ID: CVE-2024-37267**	N/A	A-KAP-STRI-020824/111
Vendor: keydatas					

CVSS 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
Product: keydatas					
Affected Version(s): * Up to (including) 2.5.2					
Unrestricted Upload of File with Dangerous Type	17-Jul-2024	9.8	The ????? (Keydatas) plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the keydatas_downloadImages function in all versions up to, and including, 2.5.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-6220**	https://plugins.trac.wordpress.org/browser/keydatas/trunk/keydatas.php	A-KEY-KEYD-020824/112
Vendor: Kibokolabs					
Product: chained_quiz					
Affected Version(s): * Up to (excluding) 1.3.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kiboko Labs Chained Quiz allows Stored XSS.This issue affects Chained	N/A	A-KIB-CHAI-020824/113

CVSS 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
			Quiz: from n/a through 1.3.2.8. **CVE ID: CVE-2024-37446**		
Vendor: kimili					
Product: kimili_flash_embed					
Affected Version(s): * Up to (including) 2.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Bester Kimili Flash Embed allows Stored XSS.This issue affects Kimili Flash Embed: from n/a through 2.5.3. **CVE ID: CVE-2024-37221**	N/A	A-KIM-KIMI-020824/114
Vendor: kraftplugins					
Product: mega_elements					
Affected Version(s): * Up to (excluding) 1.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kraftplugins Mega Elements.This issue affects Mega Elements: from n/a through 1.2.2. **CVE ID: CVE-2024-37466**	N/A	A-KRA-MEGA-020824/115

CVSS 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
Vendor: Kriesi					
Product: enfold					
Affected Version(s): * Up to (excluding) 5.6.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kriesi.At Enfold allows Reflected XSS.This issue affects Enfold: from n/a through 5.6.9. **CVE ID: CVE-2024-37199**	N/A	A-KRI-ENFO-020824/116
Vendor: kube-logging					
Product: logging-operator					
Affected Version(s): 4.6.0					
Incorrect Default Permissions	24-Jul-2024	8.8	Insecure permissions in logging-operator v4.6.0 allows attackers to access sensitive data and escalate privileges by obtaining the service account's token. **CVE ID: CVE-2024-36541**	N/A	A-KUB-LOGG-020824/117
Vendor: librechat					
Product: librechat					
Affected Version(s): * Up to (including) 0.7.3					
N/A	22-Jul-2024	9.8	LibreChat through 0.7.4-rc1 has incorrect access control for message	https://github.com/danny-avila/LibreChat/pull/3363	A-LIB-LIBR-020824/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates. (Work on a fixed version release has started in PR 3363.) **CVE ID: CVE-2024-41703**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jul-2024	9.8	LibreChat through 0.7.4-rc1 does not validate the normalized pathnames of images. (Work on a fixed version release has started in PR 3363.) **CVE ID: CVE-2024-41704**	https://github.com/danny-avila/LibreChat/pull/3363	A-LIB-LIBR-020824/119
Affected Version(s): 0.7.4					
N/A	22-Jul-2024	9.8	LibreChat through 0.7.4-rc1 has incorrect access control for message updates. (Work on a fixed version release has started in PR 3363.) **CVE ID: CVE-2024-41703**	https://github.com/danny-avila/LibreChat/pull/3363	A-LIB-LIBR-020824/120
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jul-2024	9.8	LibreChat through 0.7.4-rc1 does not validate the normalized pathnames of images. (Work on a fixed version release has started in PR 3363.) **CVE ID: CVE-2024-41704**	https://github.com/danny-avila/LibreChat/pull/3363	A-LIB-LIBR-020824/121
Vendor: Litespeedtech					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: litespeed_cache					
Affected Version(s): * Up to (excluding) 6.3					
Cross-Site Request Forgery (CSRF)	24-Jul-2024	5.4	The LiteSpeed Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.2.0.1. This is due to missing or incorrect nonce validation. This makes it possible for unauthenticated attackers to update the token setting and inject malicious JavaScript via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-3246**	https://plugins.trac.wordpress.org/changeset/3123399/litespeed-cache/trunk/src/cloud.cls.php	A-LIT-LITE-020824/122
Vendor: livemesh					
Product: beaver_builder_addons					
Affected Version(s): * Up to (excluding) 3.7					
Improper Neutralization of Input During Web Page Generation	21-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Livemesh Livemesh	N/A	A-LIV-BEAV-020824/123

CVSS 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
('Cross-site Scripting')			Addons for Beaver Builder allows Stored XSS.This issue affects Livemesh Addons for Beaver Builder: from n/a through 3.6.1. **CVE ID: CVE-2024-38784**		
Vendor: magazine3					
Product: schema_\&_structured_data_for_wp_\&_amp					
Affected Version(s): * Up to (excluding) 1.34.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	5.4	The Schema & Structured Data for WP & AMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'url' attribute within the Q&A Block widget in all versions up to, and including, 1.33 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	N/A	A-MAG-SCHE-020824/124

CVSS 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-2024-5582		
Vendor: mailster					
Product: mailster					
Affected Version(s): * Up to (excluding) 4.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in EverPress Mailster allows Reflected XSS.This issue affects Mailster: from n/a through 4.0.9. **CVE ID: CVE-2024-37433**	N/A	A-MAI-MAIL-020824/125
Vendor: Mapsmarker					
Product: leaflet_maps_marker					
Affected Version(s): * Up to (excluding) 3.12.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MapsMarker.Com e.U. Leaflet Maps Marker allows Stored XSS.This issue affects Leaflet Maps Marker: from n/a through 3.12.9. **CVE ID: CVE-2024-38782**	N/A	A-MAP-LEAF-020824/126
Vendor: Microsoft					

CVSS 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
Product: edge					
Affected Version(s): * Up to (excluding) 127.0.2651.74					
N/A	25-Jul-2024	5.9	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability **CVE ID: CVE-2024-38103**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38103	A-MIC-EDGE-020824/127
Vendor: nextscripts					
Product: social_networks_auto_poster					
Affected Version(s): * Up to (including) 4.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NextScripts allows Reflected XSS.This issue affects NextScripts: from n/a through 4.4.6. **CVE ID: CVE-2024-37275**	N/A	A-NEX-SOCI-020824/128
Vendor: nicdarkthemes					
Product: restaurant_food					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nicdark Restaurant Reservations allows Stored XSS.This issue	N/A	A-NIC-REST-020824/129

CVSS 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
			affects Restaurant Reservations: from n/a through 2.0. **CVE ID: CVE-2024-37223**		
Vendor: ninjabeaveraddon					
Product: ninja_beaver_add-ons_for_beaver_builder					
Affected Version(s): * Up to (including) 2.4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ninja Team Ninja Beaver Add-ons for Beaver Builder allows Stored XSS.This issue affects Ninja Beaver Add-ons for Beaver Builder: from n/a through 2.4.5. **CVE ID: CVE-2024-37244**	N/A	A-NIN-NINJ-020824/130
Vendor: northernbeacheswebsites					
Product: ideapush					
Affected Version(s): * Up to (excluding) 8.61					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Martin Gibson IdeaPush allows Stored XSS.This issue affects	N/A	A-NOR-IDEA-020824/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IdeaPush: from n/a through 8.60. **CVE ID: CVE-2024-37265**		
Affected Version(s): * Up to (excluding) 8.66					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Martin Gibson IdeaPush allows Stored XSS.This issue affects IdeaPush: from n/a through 8.65. **CVE ID: CVE-2024-37461**	N/A	A-NOR-IDEA-020824/132
Vendor: online_blood_bank_management_system_project					
Product: online_blood_bank_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jul-2024	9.8	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file login.php of the component Login. The manipulation of the argument user/pass leads to sql injection. The attack may be	N/A	A-ONL-ONLI-020824/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272120. **CVE ID: CVE-2024-6966**		
Vendor: online_student_management_system_project					
Product: online_student_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	17-Jul-2024	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Online Student Management System 1.0. This issue affects some unknown processing of the file /add-students.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-271703.	N/A	A-ONL-ONLI-020824/134

CVSS 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-2024-6801		
Vendor: Openstack					
Product: nova					
Affected Version(s): * Up to (excluding) 27.4.1					
N/A	24-Jul-2024	6.5	In OpenStack Nova before 27.4.1, 28 before 28.2.1, and 29 before 29.1.1, by supplying a raw format image that is actually a crafted QCOW2 image with a backing file path or VMDK flat image with a descriptor file path, an authenticated user may convince systems to return a copy of the referenced file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Nova deployments are affected. NOTE: this issue exists because of an incomplete fix for CVE-2022-47951 and CVE-2024-32498. **CVE ID: CVE-2024-40767**	https://security.openstack.org/, https://security.openstack.org/ossa/OSSA-2024-002.html	A-OPE-NOVA-020824/135
Affected Version(s): From (including) 28.0.0 Up to (excluding) 28.2.1					
N/A	24-Jul-2024	6.5	In OpenStack Nova before 27.4.1, 28 before 28.2.1, and	https://security.openstack.org/, https://security	A-OPE-NOVA-020824/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			29 before 29.1.1, by supplying a raw format image that is actually a crafted QCOW2 image with a backing file path or VMDK flat image with a descriptor file path, an authenticated user may convince systems to return a copy of the referenced file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Nova deployments are affected. NOTE: this issue exists because of an incomplete fix for CVE-2022-47951 and CVE-2024-32498. **CVE ID: CVE-2024-40767**	.openstack.org/ossa/OSSA-2024-002.html	
Affected Version(s): From (including) 29.0.0 Up to (excluding) 29.1.1					
N/A	24-Jul-2024	6.5	In OpenStack Nova before 27.4.1, 28 before 28.2.1, and 29 before 29.1.1, by supplying a raw format image that is actually a crafted QCOW2 image with a backing file path or VMDK flat image with a descriptor file path, an	https://security.openstack.org/, https://security.openstack.org/ossa/OSSA-2024-002.html	A-OPE-NOVA-020824/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user may convince systems to return a copy of the referenced file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Nova deployments are affected. NOTE: this issue exists because of an incomplete fix for CVE-2022-47951 and CVE-2024-32498. **CVE ID: CVE-2024-40767**		
Vendor: Oracle					
Product: database_server					
Affected Version(s): From (including) 19.3 Up to (including) 19.23					
N/A	16-Jul-2024	7.2	Vulnerability in the Oracle Database RDBMS Security component of Oracle Database Server. Supported versions that are affected are 19.3-19.23. Easily exploitable vulnerability allows high privileged attacker having Execute on SYS.XS_DIAG privilege with network access via Oracle Net to	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-DATA-020824/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Database RDBMS Security. Successful attacks of this vulnerability can result in takeover of Oracle Database RDBMS Security. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID: CVE-2024-21184**		
Product: financial_services_revenue_management_and_billing					
Affected Version(s): 6.0.0.0.0					
N/A	16-Jul-2024	6.1	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: Chatbot). Supported versions that are affected are 6.0.0.0.0 and 6.1.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-FINA-020824/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Financial Services Revenue Management and Billing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Revenue Management and Billing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Revenue Management and Billing accessible data as well as unauthorized read access to a subset of Oracle Financial Services Revenue Management and Billing accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

CVSS 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
			C:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2024-21188**		
Affected Version(s): 6.1.0.0.0					
N/A	16-Jul-2024	6.1	Vulnerability in the Oracle Financial Services Revenue Management and Billing product of Oracle Financial Services Applications (component: Chatbot). Supported versions that are affected are 6.0.0.0.0 and 6.1.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Revenue Management and Billing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Revenue Management and Billing, attacks may significantly impact additional products	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-FINA-020824/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Revenue Management and Billing accessible data as well as unauthorized read access to a subset of Oracle Financial Services Revenue Management and Billing accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2024-21188**		
Product: mysql_cluster					
Affected Version(s): * Up to (including) 7.5.34					
N/A	16-Jul-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21177**		
Affected Version(s): From (including) 7.6.0 Up to (including) 7.6.30					
N/A	16-Jul-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21177**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.37					
N/A	16-Jul-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21177**		
Affected Version(s): From (including) 8.1.0 Up to (including) 8.4.0					
N/A	16-Jul-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21177**		
Product: mysql_server					
Affected Version(s): 9.0.0					
N/A	16-Jul-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38, 8.4.1 and 9.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/145

CVSS 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
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21185**		
Affected Version(s): From (including) 8.1.0 Up to (including) 8.4.0					
N/A	16-Jul-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/146

CVSS 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-2024-21177		
N/A	16-Jul-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21179**	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/147
Affected Version(s): * Up to (including) 8.0.37					
N/A	16-Jul-2024	6.5	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com/security-	A-ORA-MYSQ-020824/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21177**	alerts/cpujul2024.html	
N/A	16-Jul-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.37 and prior	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21179**		
Affected Version(s): * Up to (including) 8.4.0					
N/A	16-Jul-2024	5.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.4.0 and prior. Difficult to exploit vulnerability allows low privileged attacker	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21176**		
Affected Version(s): 8.0.38					
N/A	16-Jul-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38, 8.4.1 and 9.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server.	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21185**		
Affected Version(s): 8.4.1					
N/A	16-Jul-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38, 8.4.1 and 9.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-MYSQ-020824/152

CVSS 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
			hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID: CVE-2024-21185**		
Product: peoplesoft_enterprise_peopletools					
Affected Version(s): 8.59					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-2024	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-PEOP-020824/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2024-21178**		
N/A	16-Jul-2024	4.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: OpenSearch	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-PEOP-020824/154

CVSS 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
			Dashboards). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

CVSS 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
			C:L/PR:L/UI:R/S:C/C:L/I:N/A:N). **CVE ID: CVE-2024-21180**		
Affected Version(s): 8.60					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-2024	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-PEOP-020824/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2024-21178**		
N/A	16-Jul-2024	4.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: OpenSearch Dashboards). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows low privileged attacker with network	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-PEOP-020824/156

CVSS 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
			access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N). **CVE ID: CVE-2024-21180**		
Affected Version(s): 8.61					
Improper Neutralization of Input During Web Page	16-Jul-2024	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-PEOP-020824/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			PeopleSoft (component: Portal). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of		

CVSS 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
			PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2024-21178**		
N/A	16-Jul-2024	4.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: OpenSearch Dashboards). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-PEOP-020824/158

CVSS 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 is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N). **CVE ID: CVE-2024-21180**		
Product: weblogic_server					
Affected Version(s): 12.2.1.4.0					
N/A	16-Jul-2024	9.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/159

CVSS 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
			network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID: CVE-2024-21181**		
N/A	16-Jul-2024	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/160

CVSS 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
			unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID: CVE-2024-21175**		
N/A	16-Jul-2024	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID: CVE-2024-21182**		
N/A	16-Jul-2024	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/A	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/162

CVSS 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
			C:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID: CVE-2024-21183**		
Affected Version(s): 14.1.1.0.0					
N/A	16-Jul-2024	9.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID: CVE-2024-21181**	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jul-2024	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID: CVE-2024-21175**	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/164
N/A	16-Jul-2024	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID: CVE-2024-21182**		
N/A	16-Jul-2024	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable	https://www.oracle.com/security-alerts/cpujul2024.html	A-ORA-WEBL-020824/166

CVSS 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 allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID: CVE-2024-21183**		
Vendor: oxilab					
Product: accordions					
Affected Version(s): * Up to (including) 2.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Biplob Adhikari Accordions allows Stored XSS.This issue affects Accordions: from n/a through 2.3.5.	N/A	A-OXI-ACCO-020824/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-37122		
Product: responsive_tabs					
Affected Version(s): * Up to (including) 4.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Biplob Adhikari Tabs allows Stored XSS.This issue affects Tabs: from n/a through 4.0.6. **CVE ID: CVE-2024-37120**	N/A	A-OXI-RESP-020824/168
Product: shortcode_addons					
Affected Version(s): * Up to (including) 3.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in biplob018 Shortcode Addons allows Stored XSS.This issue affects Shortcode Addons: from n/a through 3.2.5. **CVE ID: CVE-2024-37121**	N/A	A-OXI-SHOR-020824/169
Vendor: pagebuildersandwich					
Product: page_builder_sandwich					
Affected Version(s): * Up to (including) 5.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PBN Hosting SL Page Builder Sandwich – Front-End Page Builder allows Stored XSS.This issue affects Page Builder Sandwich – Front-End Page Builder: from n/a through 5.1.0. **CVE ID: CVE-2024-37219**	N/A	A-PAG-PAGE-020824/170
Vendor: payplus					
Product: payplus_payment_gateway					
Affected Version(s): * Up to (excluding) 6.6.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2024	9.8	The PayPlus Payment Gateway WordPress plugin before 6.6.9 does not properly sanitise and escape a parameter before using it in a SQL statement via a WooCommerce API route available to unauthenticated users, leading to an SQL injection vulnerability. **CVE ID: CVE-2024-6205**	N/A	A-PAY-PAYP-020824/171

CVSS 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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PayPlus LTD PayPlus Payment Gateway allows Reflected XSS.This issue affects PayPlus Payment Gateway: from n/a through 6.6.8. **CVE ID: CVE-2024-37459**	N/A	A-PAY-PAYP-020824/172
Vendor: permalink_manager_lite_project					
Product: permalink_manager_lite					
Affected Version(s): * Up to (excluding) 2.4.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Maciej Bis Permalink Manager Lite allows Reflected XSS.This issue affects Permalink Manager Lite: from n/a through 2.4.3.3. **CVE ID: CVE-2024-37257**	N/A	A-PER-PERM-020824/173
Vendor: pixelyoursite					
Product: pixelyoursite					
Affected Version(s): * Up to (excluding) 9.6.2					

CVSS 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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PixelYourSite PixelYourSite – Your smart PIXEL (TAG) Manager allows Stored XSS.This issue affects PixelYourSite – Your smart PIXEL (TAG) Manager: from n/a through 9.6.1.1. **CVE ID: CVE-2024-37447**	N/A	A-PIX-PIXE-020824/174
Vendor: print_my_blog_project					
Product: print_my_blog					
Affected Version(s): * Up to (excluding) 3.27.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Nelson Print My Blog allows Stored XSS.This issue affects Print My Blog: from n/a through 3.27.0. **CVE ID: CVE-2024-37271**	N/A	A-PRI-PRIN-020824/175
Vendor: Progress					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: telerik_reporting					
Affected Version(s): * Up to (excluding) 18.1.24.709					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	24-Jul-2024	9.8	In Progress® Telerik® Reporting versions prior to 18.1.24.709, a code execution attack is possible through object injection via an insecure type resolution vulnerability. **CVE ID: CVE-2024-6096**	https://docs.telerik.com/reporting/knowledge-base/unsafe-reflection-CVE-2024-6096	A-PRO-TELE-020824/176
Product: telerik_report_server					
Affected Version(s): * Up to (excluding) 10.1.24.709					
Deserialization of Untrusted Data	24-Jul-2024	9.8	In Progress® Telerik® Report Server versions prior to 2024 Q2 (10.1.24.709), a remote code execution attack is possible through an insecure deserialization vulnerability. **CVE ID: CVE-2024-6327**	https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-6327	A-PRO-TELE-020824/177
Vendor: projectzealous					
Product: pz_frontend_manager					
Affected Version(s): * Up to (excluding) 1.0.6					
Cross-Site Request Forgery (CSRF)	22-Jul-2024	8.8	The PZ Frontend Manager WordPress plugin before 1.0.6 does not have CSRF checks in some places, which could allow attackers to	N/A	A-PRO-PZ_F-020824/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make logged in users perform unwanted actions via CSRF attacks **CVE ID: CVE-2024-6244**		
Vendor: Proton					
Product: protonvpn					
Affected Version(s): * Up to (excluding) 3.2.10					
N/A	22-Jul-2024	9.8	ProtonVPN before 3.2.10 on Windows mishandles the drive installer path, which should use this: "" + ExpandConstant('{autopf}\Proton\Drive') + "" in Setup/setup.iss. **CVE ID: CVE-2024-37391**	https://github.com/ProtonVPN/win-app/commit/2e4e25036842aaf48838c6a59f14671b86c20aa7, https://github.com/ProtonVPN/win-app/compare/3.2.9...3.2.10	A-PRO-PROT-020824/179
Vendor: prowcplugins					
Product: empty_cart_button_for_woocommerce					
Affected Version(s): * Up to (including) 1.3.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ProWCPlugins Empty Cart Button for WooCommerce allows Stored XSS.This issue affects Empty Cart Button for WooCommerce:	N/A	A-PRO-EMPT-020824/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 1.3.8. **CVE ID: CVE-2024-37217**		
Vendor: quantumcloud					
Product: ai_chatbot					
Affected Version(s): * Up to (excluding) 5.5.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	4.8	The AI ChatBot for WordPress – WPBot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 5.5.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID: CVE-2024-6669**	https://plugins.trac.wordpress.org/changeset/3119022/	A-QUA-AI_C-020824/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Redhat					
Product: openshift_container_platform					
Affected Version(s): 3.11					
Missing Authentication for Critical Function	24-Jul-2024	6.5	A flaw was found in the Openshift console. The /API/helm/verify endpoint is tasked to fetch and verify the installation of a Helm chart from a URI that is remote HTTP/HTTPS or local. Access to this endpoint is gated by the authHandlerWithUser() middleware function. Contrary to its name, this middleware function does not verify the validity of the user's credentials. As a result, unauthenticated users can access this endpoint. **CVE ID: CVE-2024-7079**	https://access.redhat.com/security/cve/CVE-2024-7079	A-RED-OPEN-020824/182
Affected Version(s): 4.0					
Missing Authentication for Critical Function	24-Jul-2024	6.5	A flaw was found in the Openshift console. The /API/helm/verify endpoint is tasked to fetch and verify the installation of a Helm chart from a URI that is remote HTTP/HTTPS or	https://access.redhat.com/security/cve/CVE-2024-7079	A-RED-OPEN-020824/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local. Access to this endpoint is gated by the authHandlerWithUser() middleware function. Contrary to its name, this middleware function does not verify the validity of the user's credentials. As a result, unauthenticated users can access this endpoint. **CVE ID: CVE-2024-7079**		
Product: service_interconnect					
Affected Version(s): 1.0					
Improper Authentication	17-Jul-2024	5.3	A flaw was found in Skupper. When Skupper is initialized with the console-enabled and with console-auth set to Openshift, it configures the openshift oauth-proxy with a static cookie-secret. In certain circumstances, this may allow an attacker to bypass authentication to the Skupper console via a specially-crafted cookie.	https://access.redhat.com/security/cve/CVE-2024-6535	A-RED-SERV-020824/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6535		
Vendor: reputeinfosystems					
Product: bookingpress					
Affected Version(s): * Up to (excluding) 1.1.6					
N/A	17-Jul-2024	8.8	The BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin plugin for WordPress is vulnerable to Arbitrary File Read to Arbitrary File Creation in all versions up to, and including, 1.1.5 via the 'bookingpress_save_lite_wizard_settings_func' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary files that contain the content of files on the server, allowing the execution of any PHP code in those files or the exposure of sensitive information. **CVE ID: CVE-2024-6467**	https://plugins.trac.wordpress.org/changeset/3116857/bookingpress-appointment-booking/trunk/core/classes/class.bookingpress.php	A-REP-BOOK-020824/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	17-Jul-2024	8.8	The BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the bookingpress_import_data_continue_process_func function in all versions up to, and including, 1.1.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site and upload arbitrary files. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	https://plugins.trac.wordpress.org/changeset/3116857/bookingpress-appointment-booking/trunk/core/classes/class.bookingpress_import_export.php?contextall=1	A-REP-BOOK-020824/186

CVSS 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-2024-6660		
Vendor: robogallery					
Product: robo_gallery					
Affected Version(s): * Up to (excluding) 3.2.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	5.4	The Photo Gallery, Images, Slider in Rbs Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the the Gallery title field in all versions up to, and including, 3.2.19 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-3896**	https://plugins.trac.wordpress.org/changeset/3100759/robo-gallery	A-ROB-ROBO-020824/187
Vendor: royal-elementor-addons					
Product: royal_elementor_addons					
Affected Version(s): * Up to (excluding) 1.3.981					
Improper Neutralization of Input During	24-Jul-2024	5.4	The Royal Elementor Addons and Templates plugin for	https://plugins.trac.wordpress.org/changeset/3121073/royal-	A-ROY-ROYA-020824/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			WordPress is vulnerable to Stored DOM-based Cross-Site Scripting via the plugin's Magazine Grid/Slider widget in all versions up to, and including, 1.3.980 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-5818**	elementor-addons	
Vendor: sftpgo_project					
Product: sftpgo					
Affected Version(s): 2.6.2					
Authorization Bypass Through User-Controlled Key	22-Jul-2024	5.3	In SFTPGO 2.6.2, the JWT implementation lacks cerrtain security measures, such as using JWT ID (JTI) claims, nonces, and proper expiration and invalidation mechanisms.	N/A	A-SFT-SFTP-020824/189

CVSS 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-2024-40430		
Vendor: shuttur					
Product: ecommerce-laravel-bootstrap					
Affected Version(s): * Up to (excluding) 2024-07-03					
Deserialization of Untrusted Data	24-Jul-2024	8.8	A vulnerability was found in kirilkirkov Ecommerce-Laravel-Bootstrap up to 1f1097a3448ce8ec53e034ea0f70b8e2a0e64a87. It has been rated as critical. Affected by this issue is the function getCartProductsIds of the file app/Cart.php. The manipulation of the argument laraCart leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The name of the patch is a02111a674ab49f65018b31da3011b1e396f59b1. It is recommended to	https://github.com/kirilkirkov/Ecommerce-Laravel-Bootstrap/commit/a02111a674ab49f65018b31da3011b1e396f59b1, https://github.com/kirilkirkov/Ecommerce-Laravel-Bootstrap/issues/18	A-SHU-ECOM-020824/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			apply a patch to fix this issue. The identifier of this vulnerability is VDB-272348. **CVE ID: CVE-2024-7067**		
Vendor: sinatrateam					
Product: sinatra					
Affected Version(s): * Up to (including) 1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in sinatrateam Sinatra allows Stored XSS.This issue affects Sinatra: from n/a through 1.3. **CVE ID: CVE-2024-37116**	N/A	A-SIN-SINA-020824/191
Vendor: Softaculous					
Product: webuzo					
Affected Version(s): * Up to (excluding) 4.2.9					
Incorrect Comparison	25-Jul-2024	9.8	Softaculous Webuzo contains an authentication bypass vulnerability through the password reset functionality. Remote, anonymous attackers can exploit this	N/A	A-SOF-WEBU-020824/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to gain full server access as the root user. **CVE ID: CVE-2024-24621**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Jul-2024	8.8	Softaculous Webuzo contains a command injection in the password reset functionality. A remote, authenticated attacker can exploit this vulnerability to gain code execution on the system. **CVE ID: CVE-2024-24622**	N/A	A-SOF-WEBU-020824/193
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-Jul-2024	8.8	Softaculous Webuzo contains a command injection vulnerability in the FTP management functionality. A remote, authenticated attacker can exploit this vulnerability to gain code execution on the system. **CVE ID: CVE-2024-24623**	N/A	A-SOF-WEBU-020824/194
Vendor: stitionai					
Product: devika					
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a	24-Jul-2024	9.1	The snapshot_path parameter in the /api/get-browser-snapshot endpoint in stitionai devika	N/A	A-STI-DEVI-020824/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			v1 is susceptible to a path traversal attack. An attacker can manipulate the snapshot_path parameter to traverse directories and access sensitive files on the server. This can potentially lead to unauthorized access to critical system files and compromise the confidentiality and integrity of the system. **CVE ID: CVE-2024-40422**		
Vendor: student_study_center_desk_management_system_project					
Product: student_study_center_desk_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2024	4.1	A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /sscdms/classes/Users.php?f=save of the component HTTP POST Request Handler.	N/A	A-STU-STUD-020824/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument firstname/middlename/lastname/username leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-271706 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-6807**		
Vendor: stylemixthemes					
Product: masterstudy_lms					
Affected Version(s): * Up to (excluding) 3.3.24					
N/A	22-Jul-2024	8.8	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.3.24 does not prevent students from creating instructor accounts, which could be used to get access to functionalities they shouldn't have. **CVE ID: CVE-2024-5973**	N/A	A-STY-MAST-020824/197
Vendor: supersaas					
Product: supersaas					
Affected Version(s): * Up to (excluding) 2.1.10					

CVSS 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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SuperSaaS SuperSaaS – online appointment scheduling allows Stored XSS.This issue affects SuperSaaS – online appointment scheduling: from n/a through 2.1.9. **CVE ID: CVE-2024-37460**	N/A	A-SUP-SUPE-020824/198
Vendor: tailoring_management_system_project					
Product: tailoring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jul-2024	9.8	A vulnerability classified as critical has been found in itsourcecode Tailoring Management System 1.0. Affected is an unknown function of the file /staffcatadd.php. The manipulation of the argument title leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	N/A	A-TAI-TAIL-020824/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The identifier of this vulnerability is VDB-272124. **CVE ID: CVE-2024-6970**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jul-2024	9.8	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file expcatadd.php. The manipulation of the argument title leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272366 is the identifier assigned to this vulnerability. **CVE ID: CVE-2024-7081**	N/A	A-TAI-TAIL-020824/200
Vendor: takashimatsuyama					
Product: my_favorites					
Affected Version(s): * Up to (including) 1.4.1					
Improper Neutralization of Input During Web Page	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site	N/A	A-TAK-MY_F-020824/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting') vulnerability in Takashi Matsuyama My Favorites allows Stored XSS.This issue affects My Favorites: from n/a through 1.4.1. **CVE ID: CVE-2024-37114**		
Vendor: technowich					
Product: wp_ulike_-_most_advanced_wordpress_marketing_toolkit					
Affected Version(s): * Up to (excluding) 4.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	4.8	The WP ULike WordPress plugin before 4.7.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2024-6094**	N/A	A-TEC-WP_U-020824/202
Vendor: Theme4press					
Product: demo_awesome					
Affected Version(s): * Up to (excluding) 1.0.2					
Improper Neutralization of Input During	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation	N/A	A-THE-DEMO-020824/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			(XSS or 'Cross-site Scripting') vulnerability in Theme4Press Demo Awesome allows Reflected XSS.This issue affects Demo Awesome: from n/a through 1.0.1. **CVE ID: CVE-2024-37206**		
Vendor: themegrill					
Product: esteem					
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeGrill Esteem allows Stored XSS.This issue affects Esteem: from n/a through 1.5.0. **CVE ID: CVE-2024-37432**	N/A	A-THE-ESTE-020824/204
Vendor: themelooks					
Product: enter_addons					
Affected Version(s): * Up to (excluding) 2.1.7					
Improper Neutralization of Input During Web Page Generation	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in	N/A	A-THE-ENTE-020824/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			ThemeLooks Enter Addons enteraddons allows Stored XSS.This issue affects Enter Addons: from n/a through 2.1.6. **CVE ID: CVE-2024-37263**		
Vendor: Themepunch					
Product: slider_revolution					
Affected Version(s): * Up to (excluding) 6.7.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemePunch OHG Slider Revolution.This issue affects Slider Revolution: from n/a through 6.7.13. **CVE ID: CVE-2024-37449**	N/A	A-THE-SLID-020824/206
Vendor: themesgrove					
Product: all-in-one_addons_for_elementor					
Affected Version(s): * Up to (excluding) 2.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themesgrove WidgetKit allows Stored XSS.This	N/A	A-THE-ALL--020824/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects WidgetKit: from n/a through 2.5.0. **CVE ID: CVE-2024-37428**		
Vendor: themewinter					
Product: eventin					
Affected Version(s): * Up to (excluding) 4.0.5					
Missing Authorization	17-Jul-2024	4.3	The Event Manager, Events Calendar, Tickets, Registrations – Eventin plugin for WordPress is vulnerable to unauthorized data importation due to a missing capability check on the 'import_file' function in all versions up to, and including, 4.0.4. This makes it possible for authenticated attackers, with Contributor-level access and above, to import events, speakers, schedules and attendee data. **CVE ID: CVE-2024-6033**	https://plugins.trac.wordpress.org/changeset/3117477/	A-THE-EVEN-020824/208
Vendor: threeroutesmedia					
Product: elegant_themes_icons					
Affected Version(s): * Up to (including) 1.3					
Improper Neutralizat	22-Jul-2024	5.4	Improper Neutralization of	N/A	A-THR-ELEG-020824/209

CVSS 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
ion of Input During Web Page Generation ('Cross-site Scripting')			Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mayur Somani, threeroutes media Elegant Themes Icons allows Stored XSS.This issue affects Elegant Themes Icons: from n/a through 1.3. **CVE ID: CVE-2024-37100**		
Vendor: uipress					
Product: uipress_lite					
Affected Version(s): * Up to (excluding) 3.4.07					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jul-2024	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in B?i Admin 2020 UiPress lite allows SQL Injection.This issue affects UiPress lite: from n/a through 3.4.06. **CVE ID: CVE-2024-38788**	N/A	A-UIP-UIPR-020824/210
Vendor: uncannyowl					
Product: uncanny_automator					
Affected Version(s): * Up to (excluding) 5.3.0.1					
Improper Neutralization of Input During	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation	N/A	A-UNC-UNCA-020824/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			(XSS or 'Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Automator Pro allows Reflected XSS.This issue affects Uncanny Automator Pro: from n/a through 5.3. **CVE ID: CVE-2024-37117**		
Vendor: unitedthemes					
Product: shortcodes					
Affected Version(s): * Up to (excluding) 5.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in UnitedThemes Shortcodes by United Themes allows Reflected XSS.This issue affects Shortcodes by United Themes: from n/a before 5.0.5. **CVE ID: CVE-2024-37097**	N/A	A-UNI-SHOR-020824/212
Vendor: usestrict					
Product: bbpress_notify					
Affected Version(s): * Up to (excluding) 2.18.4					
Improper Neutralizat	21-Jul-2024	6.1	Improper Neutralization of	N/A	A-USE-BBPR-020824/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vinny Alves (UseStrict Consulting) bbPress Notify allows Reflected XSS.This issue affects bbPress Notify: from n/a through 2.18.3. **CVE ID: CVE-2024-37485**		
Vendor: vcita					
Product: online_booking_\&_scheduling_calendar_for_wordpress_by_vcita					
Affected Version(s): * Up to (excluding) 4.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in vCita.Com Online Booking & Scheduling Calendar for WordPress by vcita allows Reflected XSS.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.4.2. **CVE ID: CVE-2024-37262**	N/A	A-VCI-ONLI-020824/214

CVSS 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
Vendor: vsourz					
Product: all_in_one_redirection					
Affected Version(s): * Up to (including) 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vsourz Digital All In One Redirection allows Reflected XSS.This issue affects All In One Redirection: from n/a through 2.2.0. **CVE ID: CVE-2024-37245**	N/A	A-VSO-ALL_-020824/215
Vendor: wcharczuk					
Product: go-chart					
Affected Version(s): * Up to (including) 2.1.1					
Loop with Unreachable Exit Condition ('Infinite Loop')	23-Jul-2024	7.5	go-chart v2.1.1 was discovered to contain an infinite loop via the drawCanvas() function. **CVE ID: CVE-2024-40060**	N/A	A-WCH-GO-C-020824/216
Vendor: wpbeaveraddons					
Product: powerpack_lite_for_beaver_builder					
Affected Version(s): * Up to (excluding) 1.3.0.5					
Improper Neutralization of Input During Web Page Generation	22-Jul-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	N/A	A-WPB-POWE-020824/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability in Beaver Addons PowerPack Lite for Beaver Builder allows Stored XSS.This issue affects PowerPack Lite for Beaver Builder: from n/a through 1.3.0.4. **CVE ID: CVE-2024-37409**		
Vendor: wpeasypay					
Product: wp_easypay					
Affected Version(s): * Up to (excluding) 4.2.4					
Missing Authorization	24-Jul-2024	6.5	The WP EasyPay – Square for WordPress plugin for WordPress is vulnerable to unauthorized modification of datadue to a missing capability check on the wpep_square_disconnect() function in all versions up to, and including, 4.2.3. This makes it possible for unauthenticated attackers to disconnect square. **CVE ID: CVE-2024-5861**	https://plugins.trac.wordpress.org/browser/wp-easy-pay/trunk/modules/payments/square-authorization.php#L199	A-WPE-WP_E-020824/218
Vendor: wpextended					
Product: wp_extended					
Affected Version(s): * Up to (excluding) 3.0.0					

CVSS 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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Extended The Ultimate WordPress Toolkit – WP Extended allows Reflected XSS.This issue affects The Ultimate WordPress Toolkit – WP Extended: from n/a through 2.4.7. **CVE ID: CVE-2024-37259**	N/A	A-WPE-WP_E-020824/219
Vendor: wplab					
Product: wp-lister_lite_for_amazon					
Affected Version(s): * Up to (excluding) 2.6.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for Amazon allows Reflected XSS.This issue affects WP-Lister Lite for Amazon: from n/a through 2.6.16. **CVE ID: CVE-2024-37261**	N/A	A-WPL-WP-L-020824/220
Vendor: wpmudev					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: branda					
Affected Version(s): * Up to (including) 3.4.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPMU DEV Branda allows Stored XSS.This issue affects Branda: from n/a through 3.4.17. **CVE ID: CVE-2024-37239**	N/A	A-WPM-BRAN-020824/221
Vendor: wppa					
Product: wp_photo_album_plus					
Affected Version(s): * Up to (excluding) 8.8.00.003					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus allows Reflected XSS.This issue affects WP Photo Album Plus: from n/a through 8.8.00.002. **CVE ID: CVE-2024-37416**	N/A	A-WPP-WP_P-020824/222
Vendor: wpsocialrocket					
Product: social_rocket					
Affected Version(s): * Up to (excluding) 1.3.4					

CVSS 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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Social Rocket allows Reflected XSS.This issue affects Social Rocket: from n/a through 1.3.3. **CVE ID: CVE-2024-37258**	N/A	A-WPS-SOCI-020824/223
Vendor: Zohocorp					
Product: manageengine_ddi_central					
Affected Version(s): * Up to (excluding) 4002					
Use of Hard-coded Credentials	17-Jul-2024	9.8	Zohocorp ManageEngine DDI Central versions 4001 and prior were vulnerable to agent takeover vulnerability due to the hard-coded sensitive keys. **CVE ID: CVE-2024-5471**	https://www.manageengine.com/dns-dhcp-ipam/security-updates/cve-2024-5471.html	A-ZOH-MANA-020824/224
Unrestricted Upload of File with Dangerous Type	17-Jul-2024	8.8	Zohocorp ManageEngine DDI Central versions 4001 and prior were vulnerable to directory traversal vulnerability which allows the user to upload new files to the server folder. **CVE ID: CVE-2024-27311**	https://www.manageengine.com/dns-dhcp-ipam/security-updates/cve-2024-27311.html	A-ZOH-MANA-020824/225

CVSS 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
Hardware					
Vendor: Adtran					
Product: 834-5					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-2024	8.8	Adtran 834-5 11.1.0.101-202106231430, and fixed as of SmartOS Version 12.5.5.1, devices allow OS Command Injection via shell metacharacters to the Ping or Traceroute utility. **CVE ID: CVE-2024-31977**	N/A	H-ADT-834--020824/226
N/A	24-Jul-2024	8.8	AdTran SRG 834-5 HDC17600021F1 devices (with SmartOS 11.1.1.1 and fixed in Version 12.1.3.1) have SSH enabled by default, accessible both over the LAN and the Internet. During a window of time when the device is being set up, it uses a default username and password combination of admin/admin with root-level privileges. An attacker can exploit this window to gain unauthorized root access by either modifying the existing admin	N/A	H-ADT-834--020824/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account or creating a new account with equivalent privileges. This vulnerability allows attackers to execute arbitrary commands. **CVE ID: CVE-2024-31970**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-2024	7.2	AdTran 834-5 HDC17600021F1 (SmartOS 11.1.1.1) devices enable the SSH service by default and have a hidden, undocumented, hard-coded support account whose password is based on the devices MAC address. All of the devices internet interfaces share a similar MAC address that only varies in their final octet. This allows network-adjacent attackers to derive the support user's SSH password by decrementing the final octet of the connected gateway address or via the BSSID. An attacker can then execute arbitrary OS commands with	N/A	H-ADT-834--020824/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			root-level privileges. **CVE ID: CVE-2024-39345**		
Product: netvanta_3120					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	4.8	**UNSUPPORTED WHEN ASSIGNED** Multiple stored cross-site scripting (XSS) vulnerabilities on AdTran NetVanta 3120 18.01.01.00.E devices allow remote attackers to inject arbitrary JavaScript, as demonstrated by /mainPassword.html, /processIdentity.html, /public.html, /dhcp.html, /private.html, /hostname.html, /connectivity.html, /NetworkMonitor.html, /trafficMonitoringConfig.html, and /wizardMain.html. **CVE ID: CVE-2024-31971**	N/A	H-ADT-NETV-020824/229
Vendor: Tenda					
Product: o3					
Affected Version(s): 2.0					
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability classified as critical was found in Tenda O3 1.0.0.10. This	N/A	H-TEN-O3-020824/230

CVSS 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 affects the function formQosSet. The manipulation of the argument remark/ipRange/upSpeed/downSpeed/enable leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272116. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6962**		
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability, which was classified as critical, has been found in Tenda O3 1.0.0.10. This issue affects the function formexeCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has	N/A	H-TEN-O3-020824/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier VDB-272117 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6963**		
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability, which was classified as critical, was found in Tenda O3 1.0.0.10. Affected is the function fromDhcpSetSer. The manipulation of the argument dhcpEn/startIP/endIP/preDNS/altDNS/mask/gateway leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272118 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early	N/A	H-TEN-O3-020824/232

CVSS 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
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6964**		
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability has been found in Tenda O3 1.0.0.10 and classified as critical. Affected by this vulnerability is the function fromVirtualSet. The manipulation of the argument ip/localPort/publicPort/app leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272119. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6965**	N/A	H-TEN-O3-020824/233
Vendor: Tendacn					
Product: ac18					
Affected Version(s): -					

CVSS 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
Out-of-bounds Write	16-Jul-2024	9.8	Tenda AC18 V15.03.3.10_EN was discovered to contain a stack-based buffer overflow vulnerability via the deviceId parameter at ip/goform/saveParentControlInfo. **CVE ID: CVE-2024-33180**	N/A	H-TEN-AC18-020824/234
Out-of-bounds Write	16-Jul-2024	9.8	Tenda AC18 V15.03.3.10_EN was discovered to contain a stack-based buffer overflow vulnerability via the deviceId parameter at ip/goform/addWifiMacFilter. **CVE ID: CVE-2024-33182**	N/A	H-TEN-AC18-020824/235
Product: fh1201					
Affected Version(s): -					
Out-of-bounds Write	24-Jul-2024	9.8	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the PPPOEPassword parameter at ip/goform/QuickIndex.	N/A	H-TEN-FH12-020824/236

CVSS 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-2024-41459		
Out-of-bounds Write	24-Jul-2024	9.8	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the entrys parameter at ip/goform/RouteStatic. **CVE ID: CVE-2024-41460**	N/A	H-TEN-FH12-020824/237
Out-of-bounds Write	24-Jul-2024	9.8	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the list1 parameter at ip/goform/DhcpListClient. **CVE ID: CVE-2024-41461**	N/A	H-TEN-FH12-020824/238
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the page parameter at ip/goform/DhcpListClient. **CVE ID: CVE-2024-41462**	N/A	H-TEN-FH12-020824/239

CVSS 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
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the entrys parameter at ip/goform/addressNat. **CVE ID: CVE-2024-41463**	N/A	H-TEN-FH12-020824/240
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the mitInterface parameter in ip/goform/RouteStatic **CVE ID: CVE-2024-41464**	N/A	H-TEN-FH12-020824/241
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the funcpara1 parameter at ip/goform/setcfm. **CVE ID: CVE-2024-41465**	N/A	H-TEN-FH12-020824/242
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-	N/A	H-TEN-FH12-020824/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based buffer overflow vulnerability via the page parameter at ip/goform/NatStaticSetting. **CVE ID: CVE-2024-41466**		
Product: i29					
Affected Version(s): 1.0					
Use of Hard-coded Credentials	16-Jul-2024	9.8	Tenda i29V1.0 V1.0.0.5 was discovered to contain a hardcoded password for root. **CVE ID: CVE-2024-35338**	N/A	H-TEN-I29-020824/244
Vendor: totolink					
Product: a6000r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Jul-2024	9.8	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the cmd parameter in the webcmd function. **CVE ID: CVE-2024-41319**	N/A	H-TOT-A600-020824/245
Operating System					
Vendor: Adtran					
Product: 834-5_firmware					
Affected Version(s): 11.1.0.101-202106231430					

CVSS 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 Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-2024	8.8	Adtran 834-5 11.1.0.101-202106231430, and fixed as of SmartOS Version 12.5.5.1, devices allow OS Command Injection via shell metacharacters to the Ping or Traceroute utility. **CVE ID: CVE-2024-31977**	N/A	O-ADT-834--020824/246
Product: netvanta_3120_firmware					
Affected Version(s): 18.01.01.00.e					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2024	4.8	**UNSUPPORTED WHEN ASSIGNED** Multiple stored cross-site scripting (XSS) vulnerabilities on AdTran NetVanta 3120 18.01.01.00.E devices allow remote attackers to inject arbitrary JavaScript, as demonstrated by /mainPassword.html, /processIdentity.html, /public.html, /dhcp.html, /private.html, /hostname.html, /connectivity.html, /NetworkMonitor.html, /trafficMonitoringConfig.html, and /wizardMain.html.	N/A	O-ADT-NETV-020824/247

CVSS 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-2024-31971		
Product: sdg_smartos					
Affected Version(s): * Up to (excluding) 12.1.3.1					
N/A	24-Jul-2024	8.8	AdTran SRG 834-5 HDC17600021F1 devices (with SmartOS 11.1.1.1 and fixed in Version 12.1.3.1) have SSH enabled by default, accessible both over the LAN and the Internet. During a window of time when the device is being set up, it uses a default username and password combination of admin/admin with root-level privileges. An attacker can exploit this window to gain unauthorized root access by either modifying the existing admin account or creating a new account with equivalent privileges. This vulnerability allows attackers to execute arbitrary commands. **CVE ID: CVE-2024-31970**	N/A	O-ADT-SDG_-020824/248
Improper Neutralization of	24-Jul-2024	7.2	AdTran 834-5 HDC17600021F1 (SmartOS 11.1.1.1)	N/A	O-ADT-SDG_-020824/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			devices enable the SSH service by default and have a hidden, undocumented, hard-coded support account whose password is based on the devices MAC address. All of the devices internet interfaces share a similar MAC address that only varies in their final octet. This allows network-adjacent attackers to derive the support user's SSH password by decrementing the final octet of the connected gateway address or via the BSSID. An attacker can then execute arbitrary OS commands with root-level privileges. **CVE ID: CVE-2024-39345**		
Affected Version(s): * Up to (excluding) 12.5.5.1					
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Jul-2024	8.8	Adtran 834-5 11.1.0.101-202106231430, and fixed as of SmartOS Version 12.5.5.1, devices allow OS Command Injection via shell metacharacters to	N/A	O-ADT-SDG_-020824/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			the Ping or Traceroute utility. **CVE ID: CVE-2024-31977**		
Vendor: Huawei					
Product: emui					
Affected Version(s): 12.0.0					
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/251
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/252
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39670**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39674**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/254
Affected Version(s): 13.0.0					
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/255
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/256
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability will affect availability. **CVE ID: CVE-2024-39670**		
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39674**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/258
Affected Version(s): 14.0.0					
N/A	25-Jul-2024	7.1	Memory request logic vulnerability in the memory module. Impact: Successful exploitation of this vulnerability will affect integrity and availability. **CVE ID: CVE-2024-39672**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/259
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/261
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39670**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/262
N/A	25-Jul-2024	5.5	Access control vulnerability in the security verification module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39671**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/263
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability.	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-EMUI-020824/264

CVSS 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-2024-39674		
Product: harmonyos					
Affected Version(s): 2.0.0					
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/265
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/266
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39670**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/267
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module.	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39674**		
Affected Version(s): 2.1.0					
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/269
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/270
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39670**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39674**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/272
Affected Version(s): 3.0.0					
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/273
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/274
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability will affect availability. **CVE ID: CVE-2024-39670**		
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39674**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/276
Affected Version(s): 3.1.0					
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/277
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/278
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/279

CVSS 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
			synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39670**		
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39674**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/280
Affected Version(s): 4.0.0					
N/A	25-Jul-2024	7.1	Memory request logic vulnerability in the memory module. Impact: Successful exploitation of this vulnerability will affect integrity and availability. **CVE ID: CVE-2024-39672**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/281
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39673		
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/283
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39670**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/284
N/A	25-Jul-2024	5.5	Access control vulnerability in the security verification module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39671**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/285
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability will affect availability. **CVE ID: CVE-2024-39674**		
Affected Version(s): 4.2.0					
N/A	25-Jul-2024	7.1	Memory request logic vulnerability in the memory module. Impact: Successful exploitation of this vulnerability will affect integrity and availability. **CVE ID: CVE-2024-39672**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/287
N/A	25-Jul-2024	7.1	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39673**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/288
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2023-7271**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/289
N/A	25-Jul-2024	5.5	Privilege escalation vulnerability in the account	https://consumer.huawei.com/	O-HUA-HARM-020824/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39670**	en/support/bulletin/2024/7/	
N/A	25-Jul-2024	5.5	Access control vulnerability in the security verification module. Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-39671**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/291
N/A	25-Jul-2024	5.5	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID: CVE-2024-39674**	https://consumer.huawei.com/en/support/bulletin/2024/7/	O-HUA-HARM-020824/292
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 3.13					
Missing Release of Memory after Effective Lifetime	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/23752737c6a618e994f9a310ec2568881a6b49c4, https://git.kern	O-LIN-LINU-020824/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers. **CVE ID: CVE-2024-42070**	el.org/stable/c/40188a25a9847dbeb7ec67517174a835a677752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b5153848bfa1c2980f	
Affected Version(s): * Up to (excluding) 4.18					
Allocation of Resources Without Limits or Throttling	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from	https://git.kernel.org/stable/c/1095b8efbb13a6a5fa583ed373ee1ccab29da2d0, https://git.kernel.org/stable/c/14e51ea78b4cc	O-LIN-LINU-020824/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation.	acb7acb1346b9241bb790a2054c, https://git.kernel.org/stable/c/1d3e3b3aa2cbe9bc7db9a7f8673a9fa6d2990d54	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thus, there is no sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_live+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240		

CVSS 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+0x6d/0x75 Found by Linux Verification Center (linuxtesting.org) with syzkaller. **CVE ID: CVE-2024-42082**		
Affected Version(s): * Up to (excluding) 4.6					
N/A	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can contain arbitrary number of extents.	https://git.kernel.org/stable/c/320273b5649bbcee87f9e65343077189699d2a7a, https://git.kernel.org/stable/c/331d1079d58206ff7dc5518185f800b412f89bc6, https://git.kernel.org/stable/c/9ea2d1c6789722d58ec191f14f9a02518d55b6b4	O-LIN-LINU-020824/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 filesystem.		

CVSS 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
			To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2] #4 __ocfs2_abort at ffffffffc0c88387 [ocfs2]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_write at ffffffff8c1dcf14		

CVSS 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
			#15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba **CVE ID: CVE-2024-42077**		
Affected Version(s): * Up to (excluding) 4.9.307					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show When bringing down the netdevice or system shutdown, a panic can be	https://git.kernel.org/stable/c/081369ad088a76429984483b8a5f7e967a125aad, https://git.kernel.org/stable/c/3a79f380b3e10edf6caa9aac90163a5d7a282204, https://git.kernel.org/stable/c/4224cfd7fb6523f7a9d1c8bb91	O-LIN-LINU-020824/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0: Shutdown was called ... [757.937260] BUG: unable to handle kernel NULL pointer dereference at (null) [758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100 CPU: 1 COMMAND: "amsd" ... #9 [ffff89240e1a38b0	bb5df1e38eb624	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX: 0000000000001000 RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090 RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0 R13: ffff89243d874090 R14: ffff89243d874080 R15:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core] #12 [ffff89240e1a3ab8] mlx5_cmd_exec at ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8] dev_attr_show at ffffffff8f0b70e3 #20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18] kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff #25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f		

CVSS 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
			#26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START|__LINK_STATE_NOCARRIER) To prevent this scenario, we also make sure that the netdevice is present. **CVE ID: CVE-2022-48850**		
Affected Version(s): * Up to (excluding) 4.9.308					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting	https://git.kernel.org/stable/c/32813321f18d5432cec1b1a6ecc964f9ea26d565, https://git.kernel.org/stable/c/56eaacb8137ba2071ce48d4e3d91979270e139a7, https://git.kernel.org/stable/c/7315f8538db009605ffba00370678142ef00ac98	O-LIN-LINU-020824/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the following: [0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi)) [0.048183] ----------[cut here]---------- [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc3+ #35 b7b319f24073fd9a3c2aa7ad15fb7993eec0b26f [0.048247] Stack : 817f0000 00000004 327804c8 810eb050 00000000 00000004 00000000 c314fdd1 [0.048278] 830cbd64 819c0000 81800000 817f0000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			83070bf4 00000001 830cbd08 00000000 [0.048307] 00000000 00000000 815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34 [0.048361] 817f0000 818a3c00 817f0000 00000004 00000000 00000000 4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/0x140 [0.048424] [<8131c2a0>]		

CVSS 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
			dump_stack_lvl+0x60/0x80 [0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>] warn_slowpath_fmt+0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_starting+0x198/0x240 [0.048483] [<810c6514>] sched_cpu_starting+0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callback_range+0x78/0x140 [0.048510] [<8108d914>] notify_cpu_starting+0x94/0x140 [0.048523] [<8106593c>] start_secondary+0xbc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			...for each but CPU 0/boot. Basic debug printks right before the mentioned line say: [0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_starting() calculates core-scheduling parameters only once per CPU start, and it's crucial to have all the parameters filled in at that moment (at least it uses cpu_smt_mask() which in fact is `&cpu_sibling_map[cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the actual map calculation, was being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP callbacks in Linux 4.14 (see [0] for the reference). Neither me nor my brief tests couldn't find any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			yield exactly what I expected from them: [0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.org/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef **CVE ID: CVE-2022-48845**		
Affected Version(s): * Up to (excluding) 4.9.320					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE The problem I'm addressing was discovered by the LTP test covering cve-2018-1000204. A short description of what happens follows: 1) The test case issues a command code 00 (TEST	https://git.kernel.org/stable/c/270475d6d2410ec66e971bf181afe1958dad565e, https://git.kernel.org/stable/c/6bfc5377a210dbda2a237f16d94d1bd4f1335026, https://git.kernel.org/stable/c/7403f4118ab94be837ab9d770507537a8057bc63	O-LIN-LINU-020824/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UNIT READY) via the SG_IO interface with: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_DEV and a corresponding dxferp. The peculiar thing about this is that TUR is not reading from the device. 2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808 ("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this first bounce buffer is allocated with GFP_ZERO. 3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we		

CVSS 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
			prepare as if the we had a DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function virtqueue_add_split() which uses DMA_FROM_DEVICE for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we first copy back the content of the second (that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer, which contains all zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized, ain't all zeros and fails. One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all other participants are well behaved). Copying the content of the original buffer into the swiotlb buffer is the only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doubt, but allow the driver to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance impact of the extra bounce. **CVE ID: CVE-2022-48853**		
Affected Version(s): * Up to (excluding) 5.10.222					
N/A	30-Jul-2024	4.1	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accomplish this by using kfree_sensitive for buffers that	https://git.kernel.org/stable/c/23e4099bdc3c8381992f9eb975c79196d6755210, https://git.kernel.org/stable/c/28c8d274848feba552e95c5c2a7e3cfe8f15c534, https://git.kernel.org/stable/c/71dd428615375e36523f4d4f7685ddd54113646d	O-LIN-LINU-020824/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			previously held the private key. **CVE ID: CVE-2024-42229**		
Affected Version(s): * Up to (excluding) 5.15.162					
Unchecked Return Value	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into account with bpf_prog_lock_ro() set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error. **CVE ID: CVE-2024-42068**	https://git.kernel.org/stable/c/05412471beba313ecded95aa17b25fe84bb2551a, https://git.kernel.org/stable/c/7d2cc63eca0c993c99d18893214abf8f85d566d8, https://git.kernel.org/stable/c/a359696856ca9409fb97655c5a8ef0f549cb6e03	O-LIN-LINU-020824/300
Out-of-bounds Write	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address access struct rdma_restrack_entry's kern_name was	https://git.kernel.org/stable/c/782bdaf9d016582 81bc813f3f873e6258aa1fd8d, https://git.kernel.org/stable/c/8656ef8a9288d6c932654f8d3856dc4ab1cfc6b5, https://git.kernel.org/stable/c/	O-LIN-LINU-020824/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			set to KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this rdma_restrack_entry, it would cause a invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one forgotten PD release in one of the ULPs. But it is not needed anymore, so delete them. **CVE ID: CVE-2024-42080**	8ac281d42337f36cf7061cf1ea094181b84bc1a9	
Affected Version(s): * Up to (excluding) 5.15.163					
Use of Uninitialized Resource	30-Jul-2024	7.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero Avoid potentially reusing uninitialized data	https://git.kernel.org/stable/c/22ea2a7f0b64d323625950414a4496520fb33657, https://git.kernel.org/stable/c/64f86337ccfe77fe3be5a9356b0dabde23fbb074, https://git.kernel.org/stable/c/7f819a2f4fbc51	O-LIN-LINU-020824/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42225	0e088b49c79addcf1734503578	
Affected Version(s): * Up to (excluding) 5.15.29					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: bypass tiling flag check in virtual display case (v2) vkms leverages common amdgpu framebuffer creation, and also as it does not support FB modifier, there is no need to check tiling flags when initing framebuffer when virtual display is enabled. This can fix below calltrace: amdgpu 0000:00:08.0: GFX9+ requires FB check based on format modifier WARNING: CPU: 0 PID: 1023 at drivers/gpu/drm/amd/amdgpu/amd	https://git.kernel.org/stable/c/cb29021be49858059138f75d6311a7c35a9379b2, https://git.kernel.org/stable/c/e2b993302f40c4eb714ecf896dd9e1c5be7d4cd7, https://git.kernel.org/stable/c/fcd1d79aa943fff4fbaa0cce1d576995a7960699	O-LIN-LINU-020824/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gpu_display.c:1150 amdgpu_display_framebuffer_init+0x8e7/0xb40 [amdgpu] v2: check adev->enable_virtual_display instead as vkms can be enabled in bare metal as well. **CVE ID: CVE-2022-48849**		
N/A	16-Jul-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: hdmi: Unregister codec device on unbind On bind we will register the HDMI codec device but we don't unregister it on unbind, leading to a device leakage. Unregister our device at unbind. **CVE ID: CVE-2022-48852**	https://git.kernel.org/stable/c/1ed68d776246f167aee9cd79f63f089c40a5e2a3, https://git.kernel.org/stable/c/e40945ab7c7f966d0c37b7bd7b0596497dfe228d, https://git.kernel.org/stable/c/ee22082c3e2f230028afa0e22aa8773b1de3c919	O-LIN-LINU-020824/304
Affected Version(s): * Up to (excluding) 5.15.30					
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/3679ccc09d8806686d579095e	O-LIN-LINU-020824/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth: hci_core: Fix leaking sent_cmd skb sent_cmd memory is not freed before freeing hci_dev causing it to leak it contents. **CVE ID: CVE-2022-48844**	d504e045af7f7d6, https://git.kernel.org/stable/c/9473d06bd1c8da49eafb685aa95a290290c672dd, https://git.kernel.org/stable/c/dd3b1dc3dd050f1f47cd13e30073285241427 0f8	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Jul-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: ice: Fix race condition during interface enslave Commit 5dbbbd01cbba83 ("ice: Avoid RTNL lock when re-creating auxiliary device") changes a process of re-creation of aux device so ice_plug_aux_dev() is called from ice_service_task() context. This unfortunately opens a race	https://git.kernel.org/stable/c/5cb1ebdbc4342b1c2ce89516e19808d64417bdbc, https://git.kernel.org/stable/c/a9bbacc53d1f5ed8febbfdf31401d20e005f49ef, https://git.kernel.org/stable/c/e1014fc5572375658fa421531cedb6e084f477dc	O-LIN-LINU-020824/306

CVSS 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

			window that can result in dead-lock
			when interface has left LAG and immediately enters LAG again.
			
			Reproducer:
			``
			#!/bin/sh
			
			ip link add lag0 type bond mode 1 miimon 100
			ip link set lag0
			
			for n in {1..10}; do
			echo Cycle: $n
			ip link set ens7f0 master lag0
			sleep 1
			ip link set ens7f0 nomaster
			done
			``
			
			This results in:
			[20976.208697] Workqueue: ice ice_service_task [ice]
			[20976.213422] Call Trace:
			[20976.215871] __schedule+0x2d1/0x830		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[20976.219364] schedule+0x35/0xa0 [20976.222510] schedule_preempt_disabled+0xa/0x10 [20976.227043] __mutex_lock.isra.7+0x310/0x420 [20976.235071] enum_all_gids_of_dev_cb+0x1c/0x100 [ib_core] [20976.251215] ib_enum_roce_netdev+0xa4/0xe0 [ib_core] [20976.256192] ib_cache_setup_one+0x33/0xa0 [ib_core] [20976.261079] ib_register_device+0x40d/0x580 [ib_core] [20976.266139] irdma_ib_register_device+0x129/0x250 [irdma] [20976.281409] irdma_probe+0x2c1/0x360 [irdma] [20976.285691] auxiliary_bus_probe+0x45/0x70 [20976.289790] really_probe+0x1f2/0x480		

CVSS 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
			[20976.298509] driver_probe_device+0x49/0xc0 [20976.302609] bus_for_each_drv+0x79/0xc0 [20976.306448] __device_attach+0xdc/0x160 [20976.310286] bus_probe_device+0x9d/0xb0 [20976.314128] device_add+0x43c/0x890 [20976.321287] __auxiliary_device_add+0x43/0x60 [20976.325644] ice_plug_aux_dev+0xb2/0x100 [ice] [20976.330109] ice_service_task+0xd0c/0xed0 [ice] [20976.342591] process_one_work+0x1a7/0x360 [20976.350536] worker_thread+0x30/0x390 [20976.358128] kthread+0x10a/0x120 [20976.365547] ret_from_fork+0x1f/0x40 ... [20976.438030] task:ip state:D stack: 0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pid:213658 ppid:213627 flags:0x00004084 [20976.446469] Call Trace: [20976.448921] __schedule+0x2d1/0x830 [20976.452414] schedule+0x35/0xa0 [20976.455559] schedule_preempt_disabled+0xa/0x10 [20976.460090] __mutex_lock.isra.7+0x310/0x420 [20976.464364] device_del+0x36/0x3c0 [20976.467772] ice_unplug_aux_dev+0x1a/0x40 [ice] [20976.472313] ice_lag_event_handler+0x2a2/0x520 [ice] [20976.477288] notifier_call_chain+0x47/0x70 [20976.481386] __netdev_upper_dev_link+0x18b/0x280 [20976.489845] bond_enslave+0xe05/0x1790 [bonding]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[20976.494475] do_setlink+0x336/0xf50 [20976.502517] __rtnl_newlink+0x529/0x8b0 [20976.543441] rtnl_newlink+0x43/0x60 [20976.546934] rtnetlink_rcv_msg+0x2b1/0x360 [20976.559238] netlink_rcv_skb+0x4c/0x120 [20976.563079] netlink_unicast+0x196/0x230 [20976.567005] netlink_sendmsg+0x204/0x3d0 [20976.570930] sock_sendmsg+0x4c/0x50 [20976.574423] ___sys_sendmsg+0x1eb/0x250 [20976.586807] __sys_sendmsg+0x7c/0xc0 [20976.606353] __sys_sendmsg+0x57/0xa0 [20976.609930] do_syscall_64+0x5b/0x1a0 [20976.613598] entry_SYSCALL_64_after_hwframe+0x65/0xca		

CVSS 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. Command 'ip link ... set nomaster' causes that ice_plug_aux_dev() is called from ice_service_task() context, aux device is created and associated device->lock is taken. 2. Command 'ip link ... set master...' calls ice's notifier under RTNL lock and that notifier calls ice_unplug_aux_dev(). That function tries to take aux device->lock but this is already taken by ice_plug_aux_dev() in step 1 3. Later ice_plug_aux_dev() tries to take RTNL lock but this is already taken in step 2 4. Dead-lock The patch fixes this issue by following changes: - Bit ICE_FLAG_PLUG_AUX_DEV is kept to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be set during ice_plug_aux_dev() call in ice_service_task() - The bit is checked in ice_clear_rdma_cap() and only if it is not set then ice_unplug_aux_dev() is called. If it is set (in other words plugging of aux device was requested and ice_plug_aux_dev() is potentially running) then the function only clears the ---truncated--- **CVE ID: CVE-2022-48842**		
Affected Version(s): * Up to (excluding) 5.16.17					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ice: fix NULL pointer dereference in ice_update_vsi_tx_ring_stats() It is possible to do NULL pointer dereference in	https://git.kernel.org/stable/c/2397270ec97c5e3009a58ac110a25e1869e9d6ff, https://git.kernel.org/stable/c/f153546913bada41a811722f2c6d17c3243a0333	O-LIN-LINU-020824/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			routine that updates Tx ring stats. Currently only stats and bytes are updated when ring pointer is valid, but later on ring is accessed to propagate gathered Tx stats onto VSI stats. Change the existing logic to move to next ring when ring is NULL. **CVE ID: CVE-2022-48841**		
Affected Version(s): * Up to (excluding) 5.17					
Use After Free	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_buffers: Fix memory corruptions on Spectrum-4 systems The following two shared buffer operations make use of the Shared Buffer Status Register (SBSR):	https://git.kernel.org/stable/c/942901e0fc74ad4b7992ef7ca9336e68d5fd6d36, https://git.kernel.org/stable/c/bf8781ede7bd9a37c0fcabca78976e61300b5a1a, https://git.kernel.org/stable/c/bfa86a96912faa0b6142a918db88cc0c738a769e	O-LIN-LINU-020824/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			# devlink sb occupancy snapshot pci/0000:01:00.0 # devlink sb occupancy clearmax pci/0000:01:00.0 The register has two masks of 256 bits to denote on which ingress / egress ports the register should operate on. Spectrum-4 has more than 256 ports, so the register was extended by cited commit with a new 'port_page' field. However, when filling the register's payload, the driver specifies the ports as absolute numbers and not relative to the first port of the port page, resulting in memory corruptions [1]. Fix by specifying the ports relative to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the first port of the port page. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 Read of size 1 at addr ffff8881068cb00f by task devlink/1566 [...] Call Trace: <TASK> dump_stack_lvl+0xc6/0x120 print_report+0xce/0x670 kasan_report+0xd7/0x110 mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 mlxsw_devlink_sb_occ_snapshot+0x75/0xb0 devlink_nl_sb_occ_snapshot_doit+0x1f9/0x2a0		

CVSS 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
			genl_family_rcv_msg_doit+0x20c/0x300 genl_rcv_msg+0x567/0x800 netlink_rcv_skb+0x170/0x450 genl_rcv+0x2d/0x40 netlink_unicast+0x547/0x830 netlink_sendmsg+0x8d4/0xdb0 __sys_sendto+0x49b/0x510 __x64_sys_sendto+0xe5/0x1c0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [...] Allocated by task 1: kasan_save_stack+0x33/0x60		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 copy_verifier_state+0xbc2/0xfb0 do_check_common+0x2c51/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30		

CVSS 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_save_free_info+0x3b/0x60 poison_slab_object+0x109/0x170 __kasan_slab_free+0x14/0x30 kfree+0xca/0x2b0 free_verifier_state+0xce/0x270 do_check_common+0x4828/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f **CVE ID: CVE-2024-42073**		
Affected Version(s): * Up to (excluding) 5.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf	https://git.kernel.org/stable/c/4c5dc3927e17489c1cae6f48c0d5e4acb4cae01f, https://git.kernel.org/stable/c/5e4ed38eb17eaca42de57d500cc0f9668d2b6abf, https://git.kernel.org/stable/c/a2a0ebff7fdeb2f66e29335adf64b9e457300dd4	O-LIN-LINU-020824/309

CVSS 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
			include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ___sys_recvmsg+0x18a/0x620 net/socket.c:2803 __sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0xcf /0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 **CVE ID: CVE-2024-42076**		
Affected Version(s): * Up to (excluding) 5.4.185					
Concurrent Execution using Shared	16-Jul-2024	7	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0401bfb27a91d7bdd74b1635c	O-LIN-LINU-020824/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			net/mlx5: Fix a race on command flush flow Fix a refcount use after free warning due to a race on command entry. Such race occurs when one of the commands releases its last refcount and frees its index and entry while another process running command flush flow takes refcount to this command entry. The process which handles commands flush may see this command as needed to be flushed if the other process released its refcount but didn't release the index yet. Fix it by adding the needed spin lock. It fixes the following warning trace: refcount_t: addition on 0; use-after-free.	1aae57cbb128da6, https://git.kernel.org/stable/c/063bd355595428750803d8736a9bb7c8db67d42d, https://git.kernel.org/stable/c/1a4017926eeea56c7540cc41b42106746ee8a0ee	

CVSS 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
			WARNING: CPU: 11 PID: 540311 at lib/refcount.c:25 refcount_warn_saturate+0x80/0xe0 ... RIP: 0010:refcount_warn_saturate+0x80/0xe0 ... Call Trace: <TASK> mlx5_cmd_trigger_completions+0x293/0x340 [mlx5_core] mlx5_cmd_flush+0x3a/0xf0 [mlx5_core] enter_error_state+0x44/0x80 [mlx5_core] mlx5_fw_fatal_reporter_err_work+0x37/0xe0 [mlx5_core] process_one_work+0x1be/0x390 worker_thread+0x4d/0x3d0 ? rescuer_thread+0x350/0x350		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kthread+0x141/0x160 ? set_kthread_struct+0x40/0x40 ret_from_fork+0x1f/0x30 </TASK> **CVE ID: CVE-2022-48858**		
Affected Version(s): * Up to (excluding) 5.4.186					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vrr: Set VRR capable prop only if it is attached to connector VRR capable property is not attached by default to the connector It is attached only if VRR is supported. So if the driver tries to call drm core set prop function without it being attached that causes NULL dereference. **CVE ID: CVE-2022-48843**	https://git.kernel.org/stable/c/0ba557d330946c23559aaea2d51ea649fdeca98a, https://git.kernel.org/stable/c/3534c5c005ef99a1804ed50b8a72cdae254cabb5, https://git.kernel.org/stable/c/62929726ef0ec72cbbe9440c5d125d4278b99894	O-LIN-LINU-020824/311
Affected Version(s): * Up to (excluding) 6.2					

CVSS 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	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix possible double free in error handling path When auxiliary_device_add() returns error and then calls auxiliary_device_uninit(), callback function adev_release calls kfree(madev). We shouldn't call kfree(madev) again in the error handling path. Set 'madev' to NULL. **CVE ID: CVE-2024-42069**	https://git.kernel.org/stable/c/1864b8224195d0e43ddb92a8151f54f6562090cc, https://git.kernel.org/stable/c/3243e64eb4d897c3eeb48b2a7221ab5a95e1282a, https://git.kernel.org/stable/c/ed45c0a0b662079d4c0e518014cc148c753979b4	O-LIN-LINU-020824/312
Affected Version(s): * Up to (excluding) 6.6					
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp: add a null check for chip_pdev structure When acp platform device creation is	https://git.kernel.org/stable/c/98d919dfee1cc402ca29d45da642852d7c9a2301, https://git.kernel.org/stable/c/b0c39ae1cc86afe74aa2f6273ccb514f8d180cf6, https://git.kernel.org/stable/c/e158ed266fc1a	O-LIN-LINU-020824/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skipped, chip->chip_pdev value will remain NULL. Add NULL check for chip->chip_pdev structure in snd_acp_resume() function to avoid null pointer dereference. **CVE ID: CVE-2024-42074**	dfa456880fb6dabce2e5623843b	
Affected Version(s): * Up to (excluding) 6.6.37					
Unchecked Return Value	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_rox() into account with bpf_jit_binary_lock_ro() set_memory_rox() can fail, leaving memory unprotected. Check return and bail out when bpf_jit_binary_lock_ro() returns an error. **CVE ID: CVE-2024-42067**	https://git.kernel.org/stable/c/044da7ae7afd4ef60806d73654a2e6a79aa4ed7a, https://git.kernel.org/stable/c/08f6c05feb1db21653e98ca84ea04ca032d014c7, https://git.kernel.org/stable/c/9fef36cad60d4226f9d06953cd56d1d2f9119730	O-LIN-LINU-020824/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix NULL pointer dereference in gfs2_log_flush In gfs2_jindex_free(), set sdp->sd_jdesc to NULL under the log flush lock to provide exclusion against gfs2_log_flush(). In gfs2_log_flush(), check if sdp->sd_jdesc is non-NULL before dereferencing it. Otherwise, we could run into a NULL pointer dereference when outstanding glock work races with an unmount (glock_work_func -> run_queue -> do_xmote -> inode_go_sync -> gfs2_log_flush). **CVE ID: CVE-2024-42079**	https://git.kernel.org/stable/c/3429ef5f50909cee9e498c50f0c499b9397116ce, https://git.kernel.org/stable/c/35264909e9d1973ab9aaa2a1b07cda70f12bb828, https://git.kernel.org/stable/c/f54f9d5368a4e92ede7dd078a62788dae3a7c6ef	O-LIN-LINU-020824/315
Affected Version(s): * Up to (excluding) 6.6.39					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	30-Jul-2024	7	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Using uninitialized value *size when calling amdgpu_vce_cs_reloc Initialize the size before calling amdgpu_vce_cs_reloc, such as case 0x03000001. V2: To really improve the handling we would actually need to have a separate value of 0xffffffff.(Christian) **CVE ID: CVE-2024-42228**	https://git.kernel.org/stable/c/855ae72c20310e5402b2317fc537d911e87537ef, https://git.kernel.org/stable/c/88a9a467c548d0b3c7761b4fd54a68e70f9c0944, https://git.kernel.org/stable/c/f8f120b3de48b8b6bdf8988a9b334c2d61c17440	O-LIN-LINU-020824/316
Affected Version(s): * Up to (excluding) 6.8					
Improper Initialization	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: initialise nfsd_info.mutex early. nfsd_info.mutex can be dereferenced by	https://git.kernel.org/stable/c/7e8b94045bc77ce4f085ddfb9eb04e5760e66169, https://git.kernel.org/stable/c/e0011bca603c101f2a3c007bdb77f7006fa78fb1	O-LIN-LINU-020824/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			svc_pool_stats_start() immediately after the new netns is created. Currently this can trigger an oops. Move the initialisation earlier before it can possibly be dereferenced. **CVE ID: CVE-2024-42078**		
Affected Version(s): * Up to (excluding) 6.9					
N/A	29-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix may_goto with negative offset. Zac's syzbot crafted a bpf prog that exposed two bugs in may_goto. The 1st bug is the way may_goto is patched. When offset is negative it should be patched differently. The 2nd bug is in the verifier: when current state may_goto_depth is	https://git.kernel.org/stable/c/175827e04f4be53f3dfb57edf12d0d49b18fd939, https://git.kernel.org/stable/c/2b2efe1937ca9f8815884bd4dcd5b32733025103	O-LIN-LINU-020824/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			equal to visited state may_goto_depth it means there is an actual infinite loop. It's not correct to prune exploration of the program at this point. Note, that this check doesn't limit the program to only one may_goto insn, since 2nd and any further may_goto will increment may_goto_depth only in the queued state pushed for future exploration. The current state will have may_goto_depth == 0 regardless of number of may_goto insns and the verifier has to explore the program until bpf_exit. **CVE ID: CVE-2024-42072**		
Excessive Iteration	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/84b767f9e34fdb143c09e66a2a20722fc2921821, https://git.kern	O-LIN-LINU-020824/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ionic: use dev_consume_skb_ any outside of napi If we're not in a NAPI softirq context, we need to be careful about how we call napi_consume_skb( ), specifically we need to call it with budget==0 to signal to it that we're not in a safe context. This was found while running some configuration stress testing of traffic and a change queue config loop running, and this curious note popped out: [4371.402645] BUG: using smp_processor_id() in preemptible [00000000] code: ethtool/20545 [4371.402897] caller is napi_skb_cache_put +0x16/0x80	el.org/stable/c/ef7646ed49fff962e97b276f4ab91327a67eeb5a	

CVSS 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
			[4371.403120] CPU: 25 PID: 20545 Comm: ethtool Kdump: loaded Tainted: G OE 6.10.0-rc3-netnext+ #8 [4371.403302] Hardware name: HPE ProLiant DL360 Gen10/ProLiant DL360 Gen10, BIOS U32 01/23/2021 [4371.403460] Call Trace: [4371.403613] <TASK> [4371.403758] dump_stack_lvl+0x4f/0x70 [4371.403904] check_preemption_disabled+0xc1/0xe0 [4371.404051] napi_skb_cache_put+0x16/0x80 [4371.404199] ionic_tx_clean+0x18a/0x240 [ionic] [4371.404354] ionic_tx_cq_service+0xc4/0x200 [ionic] [4371.404505] ionic_tx_flush+0x15/0x70 [ionic] [4371.404653] ? ionic_lif_qcq_deinit.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			isra.23+0x5b/0x70 [ionic] [4371.404805] ionic_txrx_deinit+0x71/0x190 [ionic] [4371.404956] ionic_reconfigure_queues+0x5f5/0xff0 [ionic] [4371.405111] ionic_set_ringparam+0x2e8/0x3e0 [ionic] [4371.405265] ethnl_set_rings+0x1f1/0x300 [4371.405418] ethnl_default_set_doit+0xbb/0x160 [4371.405571] genl_family_rcv_msg_doit+0xff/0x130 [...] I found that ionic_tx_clean() calls napi_consume_skb() which calls napi_skb_cache_put(), but before that last call is the note /* Zero budget indicate non-NAPI context called us, like netpoll */ and DEBUG_NET_WAR		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			N_ON_ONCE(!in_softirq()); Those are pretty big hints that we're doing it wrong. We can pass a context hint down through the calls to let ionic_tx_clean() know what we're doing so it can call napi_consume_skb() correctly. **CVE ID: CVE-2024-42071**		
Use After Free	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix remap of arena. The bpf arena logic didn't account for mremap operation. Add a refcnt for multiple mmap events to prevent use-after-free in arena_vm_close. **CVE ID: CVE-2024-42075**	https://git.kernel.org/stable/c/87496a1b01e8e2e399428c0db25e106f7961d01e, https://git.kernel.org/stable/c/b90d77e5fd784ada62ddd714d15ee2400c28e1cf	O-LIN-LINU-020824/320
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/8ae401525ae84228a8986bb369224a6224e4d	O-LIN-LINU-020824/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ionic: fix kernel panic due to multi-buffer handling Currently, the ionic_run_xdp() doesn't handle multi-buffer packets properly for XDP_TX and XDP_REDIRECT. When a jumbo frame is received, the ionic_run_xdp() first makes xdp frame with all necessary pages in the rx descriptor. And if the action is either XDP_TX or XDP_REDIRECT, it should unmap dma-mapping and reset page pointer to NULL for all pages, not only the first page. But it doesn't for SG pages. So, SG pages unexpectedly will be reused. It eventually causes kernel panic. Oops: general protection fault, probably for non-canonical address	22f, https://git.kernel.org/stable/c/e3f02f32a05009a688a87f5799e049ed6b55bab5	

CVSS 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
			0x504f4e4dbebc64ff: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 0 Comm: swapper/3 Not tainted 6.10.0-rc3+ #25 RIP: 0010:xdp_return_frame+0x42/0x90 Code: 01 75 12 5b 4c 89 e6 5d 31 c9 41 5c 31 d2 41 5d e9 73 fd ff ff 44 8b 6b 20 0f b7 43 0a 49 81 ed 68 01 00 00 49 29 c5 49 01 fd <41> 80 7d0 RSP: 0018:ffff99d00122ce08 EFLAGS: 00010202 RAX: 0000000000005453 RBX: ffff8d325f904000 RCX: 0000000000000001 RDX: 00000000670e1000 RSI: 000000011f90d000 RDI: 504f4e4d4c4b4a49 RBP: ffff99d003907740 R08: 0000000000000000 R09:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 R10: 000000011f90d000 R11: 0000000000000000 R12: ffff8d325f904010 R13: 504f4e4dbebc64fd R14: ffff8d3242b070c8 R15: ffff99d0039077c0 FS: 0000000000000000(0000) GS:ffff8d399f780000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f41f6c85e38 CR3: 000000037ac30000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <IRQ> ? die_addr+0x33/0x90		

CVSS 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_general_protection+0x251/0x2f0 ? asm_exc_general_protection+0x22/0x30 ? xdp_return_frame+0x42/0x90 ionic_tx_clean+0x211/0x280 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_tx_cq_service+0xd3/0x210 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_txrx_napi+0x41/0x1b0 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] __napi_poll.constprop.0+0x29/0x1b0 net_rx_action+0x2c4/0x350 handle_softirqs+0xf4/0x320 irq_exit_rcu+0x78/0xa0		

CVSS 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
			common_interrupt +0x77/0x90 **CVE ID: CVE-2024-42083**		
Affected Version(s): * Up to (excluding) 6.9.8					
N/A	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip pipe if the pipe idx not set properly [why] Driver crashes when pipe idx not set properly [how] Add code to skip the pipe that idx not set properly **CVE ID: CVE-2024-42064**	https://git.kernel.org/stable/c/27df59c6071470efce7182ee92fbb16afba551e0, https://git.kernel.org/stable/c/af114efe8d24b5711cfbedf7180f2ac1a296c24b	O-LIN-LINU-020824/322
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add a NULL check in xe_ttm_stolen_mgr_init Add an explicit check to ensure	https://git.kernel.org/stable/c/a6eff8f9c7e844cb24ccb188ca24abcd59734e74, https://git.kernel.org/stable/c/cc796a77985d6af75c9362cb2e73dce4ae3f97cd	O-LIN-LINU-020824/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that the mgr is not NULL. **CVE ID: CVE-2024-42065**		
Integer Overflow or Wraparound	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix potential integer overflow in page size calculation Explicitly cast tbo->page_alignment to u64 before bit-shifting to prevent overflow when assigning to min_page_size. **CVE ID: CVE-2024-42066**	https://git.kernel.org/stable/c/4f4fcafde343a54465f85a2909fc684918507a4b, https://git.kernel.org/stable/c/79d54ddf0e292b810887994bb04709c5ac0e1531	O-LIN-LINU-020824/324
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_devcoredump: Check NULL before assignments Assign 'xe_devcoredump_snapshot *' and 'xe_device *' only if 'coredump' is not NULL.	https://git.kernel.org/stable/c/76ec0e33707282d5321555698d902f4e067aff37, https://git.kernel.org/stable/c/b15e65349553b1689d15fbdebea874ca5ae2274a	O-LIN-LINU-020824/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v2 - Fix commit messages. v3 - Define variables before code.(Ashutosh/Jose) v4 - Drop return check for coredump_to_xe. (Jose/Rodrigo) v5 - Modify misleading commit message. (Matt) **CVE ID: CVE-2024-42081**		
Affected Version(s): * Up to (excluding) 6.9.9					
N/A	30-Jul-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix overlapping copy within dml_core_mode_programming [WHY] &mode_lib->mp.Watermark	https://git.kernel.org/stable/c/9342da15f2491d8600eca89c8e0da08876fb969b, https://git.kernel.org/stable/c/f1fd8a0a54e6d23a6d16ee29159f247862460fd1	O-LIN-LINU-020824/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and &locals->Watermark are the same address. memcpy may lead to unexpected behavior. [HOW] memmove should be used. **CVE ID: CVE-2024-42227**		
Affected Version(s): 5.17					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ice: fix NULL pointer dereference in ice_update_vsi_tx_ring_stats() It is possible to do NULL pointer dereference in routine that updates Tx ring stats. Currently only stats and bytes are updated when ring pointer is valid, but later on ring is accessed to propagate gathered Tx stats onto VSI stats.	https://git.kernel.org/stable/c/2397270ec97c5e3009a58ac110a25e1869e9d6ff, https://git.kernel.org/stable/c/f153546913bada41a811722f2c6d17c3243a0333	O-LIN-LINU-020824/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Change the existing logic to move to next ring when ring is NULL. **CVE ID: CVE-2022-48841**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Jul-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: ice: Fix race condition during interface enslave Commit 5dbbbd01cbba83 ("ice: Avoid RTNL lock when re-creating auxiliary device") changes a process of re-creation of aux device so ice_plug_aux_dev() is called from ice_service_task() context. This unfortunately opens a race window that can result in dead-lock when interface has left LAG and immediately enters LAG again.	https://git.kernel.org/stable/c/5cb1ebdbc4342b1c2ce89516e19808d64417bdbc, https://git.kernel.org/stable/c/a9bbacc53d1f5ed8febbfdf31401d20e005f49ef, https://git.kernel.org/stable/c/e1014fc5572375658fa421531cedb6e084f477dc	O-LIN-LINU-020824/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			Reproducer:
			``
			#!/bin/sh
			
			ip link add lag0 type bond mode 1 miimon 100
			ip link set lag0
			
			for n in {1..10}; do
			echo Cycle: $n
			ip link set ens7f0 master lag0
			sleep 1
			ip link set ens7f0 nomaster
			done
			``
			
			This results in:
			[20976.208697] Workqueue: ice ice_service_task [ice]
			[20976.213422] Call Trace:
			[20976.215871] __schedule+0x2d1/0x830
			[20976.219364] schedule+0x35/0xa0
			[20976.222510] schedule_preempt_disabled+0xa/0x10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[20976.227043] __mutex_lock.isra.7 +0x310/0x420 [20976.235071] enum_all_gids_of_d ev_cb+0x1c/0x100 [ib_core] [20976.251215] ib_enum_roce_netd ev+0xa4/0xe0 [ib_core] [20976.256192] ib_cache_setup_one +0x33/0xa0 [ib_core] [20976.261079] ib_register_device+ 0x40d/0x580 [ib_core] [20976.266139] irdma_ib_register_ device+0x129/0x2 50 [irdma] [20976.281409] irdma_probe+0x2c 1/0x360 [irdma] [20976.285691] auxiliary_bus_prob e+0x45/0x70 [20976.289790] really_probe+0x1f2 /0x480 [20976.298509] driver_probe_devic e+0x49/0xc0 [20976.302609] bus_for_each_drv+ 0x79/0xc0		

CVSS 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
			[20976.306448] __device_attach+0xdc/0x160 [20976.310286] bus_probe_device+0x9d/0xb0 [20976.314128] device_add+0x43c/0x890 [20976.321287] __auxiliary_device_add+0x43/0x60 [20976.325644] ice_plug_aux_dev+0xb2/0x100 [ice] [20976.330109] ice_service_task+0xd0c/0xed0 [ice] [20976.342591] process_one_work+0x1a7/0x360 [20976.350536] worker_thread+0x30/0x390 [20976.358128] kthread+0x10a/0x120 [20976.365547] ret_from_fork+0x1f/0x40 ... [20976.438030] task:ip state:D stack: 0 pid:213658 ppid:213627 flags:0x00004084 [20976.446469] Call Trace:		

CVSS 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
			[20976.448921] __schedule+0x2d1/0x830 [20976.452414] schedule+0x35/0xa0 [20976.455559] schedule_preempt_disabled+0xa/0x10 [20976.460090] __mutex_lock.isra.7+0x310/0x420 [20976.464364] device_del+0x36/0x3c0 [20976.467772] ice_unplug_aux_dev+0x1a/0x40 [ice] [20976.472313] ice_lag_event_handler+0x2a2/0x520 [ice] [20976.477288] notifier_call_chain+0x47/0x70 [20976.481386] __netdev_upper_dev_link+0x18b/0x280 [20976.489845] bond_enslave+0xe05/0x1790 [bonding] [20976.494475] do_setlink+0x336/0xf50 [20976.502517] __rtnl_newlink+0x529/0x8b0		

CVSS 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
			[20976.543441] rtnl_newlink+0x43/0x60 [20976.546934] rtnetlink_rcv_msg+0x2b1/0x360 [20976.559238] netlink_rcv_skb+0x4c/0x120 [20976.563079] netlink_unicast+0x196/0x230 [20976.567005] netlink_sendmsg+0x204/0x3d0 [20976.570930] sock_sendmsg+0x4c/0x50 [20976.574423] ___sys_sendmsg+0x1eb/0x250 [20976.586807] __sys_sendmsg+0x7c/0xc0 [20976.606353] __sys_sendmsg+0x57/0xa0 [20976.609930] do_syscall_64+0x5b/0x1a0 [20976.613598] entry_SYSCALL_64_after_hwframe+0x65/0xca 1. Command 'ip link ... set nomaster' causes that ice_plug_aux_dev()		

CVSS 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 called from ice_service_task() context, aux device is created and associated device->lock is taken. 2. Command 'ip link ... set master...' calls ice's notifier under RTNL lock and that notifier calls ice_unplug_aux_dev(). That function tries to take aux device->lock but this is already taken by ice_plug_aux_dev() in step 1 3. Later ice_plug_aux_dev() tries to take RTNL lock but this is already taken in step 2 4. Dead-lock The patch fixes this issue by following changes: - Bit ICE_FLAG_PLUG_AUX_DEV is kept to be set during ice_plug_aux_dev() call in ice_service_task()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			- The bit is checked in ice_clear_rdma_cap () and only if it is not set then ice_unplug_aux_dev () is called. If it is set (in other words plugging of aux device was requested and ice_plug_aux_dev() is potentially running) then the function only clears the ---truncated--- **CVE ID: CVE-2022-48842**		
Affected Version(s): 6.10					
Incorrect Calculation	30-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix calc_available_free_space() for zoned mode calc_available_free_space() returns the total size of metadata (or system) block groups, which can be allocated from unallocated disk	https://git.kernel.org/stable/c/64d2c847ba380e07b9072d65a50aa6469d2aa43f, https://git.kernel.org/stable/c/8548903b1999bba02a2b894ad750ab8eb1f40307	O-LIN-LINU-020824/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			space. The logic is wrong on zoned mode in two places. First, the calculation of data_chunk_size is wrong. We always allocate one zone as one chunk, and no partial allocation of a zone. So, we should use zone_size (= data_sinfo->chunk_size) as it is. Second, the result "avail" may not be zone aligned. Since we always allocate one zone as one chunk on zoned mode, returning non-zone size aligned bytes will result in less pressure on the async metadata reclaim process. This is serious for the nearly full state with a large zone size device. Allowing over-commit too much		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will result in less async reclaim work and end up in ENOSPC. We can align down to the zone size to avoid that. **CVE ID: CVE-2024-42231**		
N/A	30-Jul-2024	4.4	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with kexec kexec on pseries disables AIL (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can execute scv instructions after AIL is disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to disable	https://git.kernel.org/stable/c/21a741eb75f80397e5f7d3739e24d7d75e619011, https://git.kernel.org/stable/c/8c6506616386ce37e59b2745fc481c6713fae4f3, https://git.kernel.org/stable/c/c550679d604798d9fed8a5b2bb5693448a25407c	O-LIN-LINU-020824/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AIL after other CPUs have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head code probably couldn't easily deal with implementing such high addresses so it was just decided not to support that interrupt at all. **CVE ID: CVE-2024-42230**		
Affected Version(s): From (including) 2.6.14 Up to (excluding) 4.9.308					
Out-of-bounds Read	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg() syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations,	https://git.kernel.org/stable/c/268dcf1f7b3193bc446ec3d14e08a240e9561e4d, https://git.kernel.org/stable/c/70b7b3c055fd4a464da8da55ff4c1f84269f9b02, https://git.kernel.org/stable/c/a055f5f2841f7522b44a2b1eccb1951b4b03d51a	O-LIN-LINU-020824/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tpacket_rcv() is queueing skbs with garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tainted 5.17.0-rc7-syzkaller-02396-g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+0x13d/0x180 mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline] packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ___sys_recvmsg+0x2c4/0x600 net/socket.c:2632 __sys_recvmsg+0x127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704		

CVSS 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
			do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 000000002000050		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ___sys_recvmsg+0x0/0x600 include/linux/uio.h:246 this frame has 1 object: [32, 160) 'addr'		

CVSS 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
			Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 >ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ========== ========== ========== ========== ====== **CVE ID: CVE-2022-48839**		
Affected Version(s): From (including) 2.6.27 Up to (excluding) 5.10.106					
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/640445d6fc059d4514ffea79eb4196299e0e2d0f,	O-LIN-LINU-020824/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mISDN: Fix memory leak in dsp_pipeline_build() dsp_pipeline_build() allocates dup pointer by kstrdup(cfg), but then it updates dup variable by strsep(&dup, "|"). As a result when it calls kfree(dup), the dup variable contains NULL. Found by Linux Driver Verification project (linuxtesting.org) with SVACE. **CVE ID: CVE-2022-48863**	https://git.kernel.org/stable/c/7777b1f795af1bb43867375d8a776080111aae1b, https://git.kernel.org/stable/c/a3d5fcc6cf2ecbba5a269631092570aa285a24cb	
Affected Version(s): From (including) 2.6.34 Up to (excluding) 4.9.307					
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount	https://git.kernel.org/stable/c/1852854ee349881efb78ccdbbb237838975902e4, https://git.kernel.org/stable/c/5e7c402892e189a7bc152b125e72261154aa585d, https://git.kernel.org/stable/c/669172ce976608b25a2f76f3c	O-LIN-LINU-020824/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do. **CVE ID: CVE-2022-48860**	65d47f042d125c9	
Affected Version(s): From (including) 3.1 Up to (excluding) 4.9.308					
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug: BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-	https://git.kernel.org/stable/c/00bdd9bf1ac6d401ad926d3d8df41b9f1399f646, https://git.kernel.org/stable/c/16b1941eac2bd499f065a6739a40ce0011a3d740, https://git.kernel.org/stable/c/2015c23610cd0efadaeca4d3a8d1dae9a45aa35a	O-LIN-LINU-020824/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syzkaller-00229-g4f12b742eb2b #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 dev_uevent+0x712/0x780 drivers/base/core.c:2320 uevent_show+0x1b8/0x380		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			drivers/base/core.c:2391
			
			dev_attr_show+0x4b/0x90 drivers/base/core.c:2094
			
			Although the bug manifested in the driver core, the real cause was a race with the gadget core. dev_uevent() does:
			
			if (dev->driver)
			
			add_uevent_var(env, "DRIVER=%s", dev->driver->name);
			
			and between the test and the dereference of dev->driver, the gadget core sets dev->driver to NULL.
			
			The race wouldn't occur if the gadget core registered its devices on a real bus, using the standard synchronization techniques of the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver core. However, it's not necessary to make such a large change in order to fix this bug; all we need to do is make sure that udc->dev.driver is always NULL. In fact, there is no reason for udc->dev.driver ever to be set to anything, let alone to the value it currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC. This patch simply removes the statements in the gadget core that touch udc->dev.driver. **CVE ID: CVE-2022-48838**		
Affected Version(s): From (including) 3.12 Up to (excluding) 4.9.307					
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1fb9dd3787495b4deb0efe66c58306b65691a48f,	O-LIN-LINU-020824/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			staging: gdm724x: fix use after free in gdm_lte_rx() The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len. **CVE ID: CVE-2022-48851**	https://git.kernel.org/stable/c/403e3afe241b62401de1f8629c9c6b9b3d69dbff, https://git.kernel.org/stable/c/48ecdf3e29a6e514e8196691589c7dfc6c4ac169	
Affected Version(s): From (including) 3.13 Up to (excluding) 4.9.307					
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in port100_send_complete Syzbot reported UAF in port100_send_complete(). The root case is in missing usb_kill_urb() calls on error handling path of ->probe function. port100_send_complete() accesses devm allocated memory which will be	https://git.kernel.org/stable/c/0e721b8f2ee5e11376dd55363f9ccb539d754b8a, https://git.kernel.org/stable/c/205c4ec78e71cbf561794e6043da80e7bae6790f, https://git.kernel.org/stable/c/2b1c85f56512d49e43bc53741fce2f508cd90029	O-LIN-LINU-020824/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			freed on probe failure. We should kill this urbs before returning an error from probe function to prevent reported use-after-free Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540 by task ksoftirqd/2/26 ... Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255		

CVSS 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_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ... Allocated by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ___kasan_kmalloc mm/kasan/common.c:515 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			___kasan_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524 alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320 drivers/nfc/port100.c:1502 Freed by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/kasan/generic.c:370 ___kasan_slab_free mm/kasan/common.c:366 [inline] ___kasan_slab_free+0xff/0x140 mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501 devres_release_all+0x114/0x190 drivers/base/devres.c:530 really_probe+0x626/0xcc0 drivers/base/dd.c:670 **CVE ID: CVE-2022-48857**		
Affected Version(s): From (including) 3.14 Up to (excluding) 4.19.317					
Missing Release of Memory after	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/23752737c6a618e994f9a310e	O-LIN-LINU-020824/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers. **CVE ID: CVE-2024-42070**	c2568881a6b49c4, https://git.kernel.org/stable/c/40188a25a9847dbeb7ec67517174a835a677752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b5153848bfa1c2980f	
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.272					
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1fb9dd3787495b4deb0efe66c58306b65691a48f, https://git.kernel.org/stable/c/	O-LIN-LINU-020824/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			staging: gdm724x: fix use after free in gdm_lte_rx() The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len. **CVE ID: CVE-2022-48851**	403e3afe241b62401de1f8629c9c6b9b3d69dbff, https://git.kernel.org/stable/c/48ecdf3e29a6e514e8196691589c7dfc6c4ac169	
Missing Release of Memory after Effective Lifetime	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: sctp: fix kernel-infoleak for SCTP sockets syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill() calls inet_diag_msg_common_fill() Make sure to clear idiag_timer/idiag_retrans/idiag_expires	https://git.kernel.org/stable/c/1502f15b9f29c41883a6139f2923523873282a83, https://git.kernel.org/stable/c/2d8fa3fdf4542a2174a72d92018f488d65d848c5, https://git.kernel.org/stable/c/3fc0fd724d199e061432b66a8d85b7d48fe485f7	O-LIN-LINU-020824/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline] copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h:162 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			simple_copy_to_iter +0xf3/0x140 net/core/datagram .c:519 __skb_datagram_ite r+0x2d5/0x11b0 net/core/datagram .c:425 skb_copy_datagram _iter+0xdc/0x270 net/core/datagram .c:533 skb_copy_datagram _msg include/linux/skbu ff.h:3696 [inline] netlink_recvmsg+0 x669/0x1c80 net/netlink/af_netl ink.c:1977 sock_recvmsg_nose c net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x 795/0xa10 net/socket.c:2097 __do_sys_recvfrom net/socket.c:2115 [inline]		

CVSS 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_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom +0x19d/0x210 net/socket.c:2111 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_post_alloc_hook mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline] __kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline] __alloc_skb+0x545/0xf90		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline] inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341 sock_diag_rcv_msg+0x24a/0x620 netlink_rcv_skb+0x40c/0x7e0 net/netlink/af_netlink.c:2494 sock_diag_rcv+0x63/0x80 net/core/sock_diag.c:277 netlink_unicast_kernel		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netlink/af_netlink.c:1317 [inline] netlink_unicast+0x1093/0x1360 net/netlink/af_netlink.c:1343 netlink_sendmsg+0x14d9/0x1720 net/netlink/af_netlink.c:1919 sock_sendmsg_nosec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline] sock_write_iter+0x594/0x690 net/socket.c:1061 do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851 vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00 fs/read_write.c:967		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120 fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000 Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not tainted 5.17.0-rc4-syzkaller #0		

CVSS 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
			Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 **CVE ID: CVE-2022-48855**		
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show When bringing down the netdevice or system shutdown, a panic can be triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0: Shutdown was called	https://git.kernel.org/stable/c/081369ad088a76429984483b8a5f7e967a125aad, https://git.kernel.org/stable/c/3a79f380b3e10edf6caa9aac90163a5d7a282204, https://git.kernel.org/stable/c/4224cfd7fb6523f7a9d1c8bb91bb5df1e38eb624	O-LIN-LINU-020824/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			... [757.937260] BUG: unable to handle kernel NULL pointer dereference at (null) [758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100 CPU: 1 COMMAND: "amsd" ... #9 [ffff89240e1a38b0] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX: 0000000000001000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090 RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0 R13: ffff89243d874090 R14: ffff89243d874080 R15: 0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core] #12 [ffff89240e1a3ab8] mlx5_cmd_exec at		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08] mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8] dev_attr_show at ffffffff8f0b70e3		

CVSS 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
			#20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18] kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff #25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f #26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START| __LINK_STATE_NOCARRIER) To prevent this scenario, we also		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make sure that the netdevice is present. **CVE ID: CVE-2022-48850**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in port100_send_complete Syzbot reported UAF in port100_send_complete(). The root case is in missing usb_kill_urb() calls on error handling path of ->probe function. port100_send_complete() accesses devm allocated memory which will be freed on probe failure. We should kill this urbs before returning an error from probe function to prevent reported use-after-free	https://git.kernel.org/stable/c/0e721b8f2ee5e11376dd55363f9ccb539d754b8a, https://git.kernel.org/stable/c/205c4ec78e71cbf561794e6043da80e7bae6790f, https://git.kernel.org/stable/c/2b1c85f56512d49e43bc53741fce2f508cd90029	O-LIN-LINU-020824/341

CVSS 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
			Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540 by task ksoftirqd/2/26 ... Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459		

CVSS 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
			port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ... Allocated by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ___kasan_kmalloc mm/kasan/common.c:515 [inline] ___kasan_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320 drivers/nfc/port100.c:1502 Freed by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370 ___kasan_slab_free mm/kasan/common.c:366 [inline] ___kasan_slab_free+0xff/0x140		

CVSS 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
			mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501 devres_release_all+0x114/0x190 drivers/base/devres.c:530 really_probe+0x626/0xcc0 drivers/base/dd.c:670 **CVE ID: CVE-2022-48857**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount	https://git.kernel.org/stable/c/1852854ee349881efb78ccdbbb237838975902e4, https://git.kernel.org/stable/c/5e7c402892e189a7bc152b125e72261154aa585d, https://git.kernel.org/stable/c/	O-LIN-LINU-020824/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do. **CVE ID: CVE-2022-48860**	669172ce976608b25a2f76f3c65d47f042d125c9	
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.273					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb() which is caused by wrong endpoint type. There was a check for the number of endpoints, but not for the type of endpoint. Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints	https://git.kernel.org/stable/c/35069e654bcab567ff8b9f0e68e1caf82c15dcd7, https://git.kernel.org/stable/c/5600f6986628dde888173409058847 4f54a540a8, https://git.kernel.org/stable/c/57277a8b5d881e02051ba9d7f6cb3f915c229821	O-LIN-LINU-020824/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fail log: usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ... Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/input/input.c:629 kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593 **CVE ID: CVE-2022-48836**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug: BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-syzkaller-00229-g4f12b742eb2b #0	https://git.kernel.org/stable/c/00bdd9bf1ac6d401ad926d3d8df41b9f1399f646, https://git.kernel.org/stable/c/16b1941eac2bd499f065a6739a40ce0011a3d740, https://git.kernel.org/stable/c/2015c23610cd0efadaeca4d3a8d1dae9a45aa35a	O-LIN-LINU-020824/344

CVSS 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
			Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 dev_uevent+0x712/0x780 drivers/base/core.c:2320 uevent_show+0x1b8/0x380 drivers/base/core.c:2391 dev_attr_show+0x4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			b/0x90 drivers/base/core.c:2094
			
			Although the bug manifested in the driver core, the real cause was a
			race with the gadget core. dev_uevent() does:
			
			if (dev->driver)
			
			add_uevent_var(env, "DRIVER=%s", dev->driver->name);
			
			and between the test and the dereference of dev->driver, the gadget
			core sets dev->driver to NULL.
			
			The race wouldn't occur if the gadget core registered its devices on
			a real bus, using the standard synchronization techniques of the
			driver core. However, it's not necessary to make such a large change		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in order to fix this bug; all we need to do is make sure that udc->dev.driver is always NULL. In fact, there is no reason for udc->dev.driver ever to be set to anything, let alone to the value it currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC. This patch simply removes the statements in the gadget core that touch udc->dev.driver. **CVE ID: CVE-2022-48838**		
Out-of-bounds Read	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg()	https://git.kernel.org/stable/c/268dcf1f7b3193bc446ec3d14e08a240e9561e4d, https://git.kernel.org/stable/c/70b7b3c055fd4a464da8da55ff4c1f84269f9b0	O-LIN-LINU-020824/345

CVSS 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
			syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations, tpacket_rcv() is queueing skbs with garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr	2, https://git.kernel.org/stable/c/a055f5f2841f7522b44a2b1eccb1951b4b03d51a	

CVSS 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
			ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not tainted 5.17.0-rc7-syzkaller-02396-g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0x13d/0x180 mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline] packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ___sys_recvmsg+0x2c4/0x600 net/socket.c:2632 ___sys_recvmsg+0x		

CVSS 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
			127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX:		

CVSS 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
			0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 0000000020000500 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ___sys_recvmsg+0x0/0x600		

CVSS 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
			include/linux/uio.h :246 this frame has 1 object: [32, 160) 'addr' Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 >ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ========== ========== ========== ========== ====== **CVE ID: CVE-2022-48839**		

CVSS 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
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting the following: [0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi)) [0.048183] ----------[cut here]---------- [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc3+	https://git.kernel.org/stable/c/32813321f18d5432cec1b1a6ecc964f9ea26d565, https://git.kernel.org/stable/c/56eaacb8137ba2071ce48d4e3d91979270e139a7, https://git.kernel.org/stable/c/7315f8538db009605ffba00370678142ef00ac98	O-LIN-LINU-020824/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#35 b7b319f24073fd9a 3c2aa7ad15fb7993 eec0b26f [0.048247] Stack : 817f0000 00000004 327804c8 810eb050 00000000 00000004 00000000 c314fdd1 [0.048278] 830cbd64 819c0000 81800000 817f0000 83070bf4 00000001 830cbd08 00000000 [0.048307] 00000000 00000000 815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34 [0.048361] 817f0000		

CVSS 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
			818a3c00 817f0000 00000004 00000000 00000000 4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/0x140 [0.048424] [<8131c2a0>] dump_stack_lvl+0x60/0x80 [0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>] warn_slowpath_fmt+0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_starting+0x198/0x240 [0.048483] [<810c6514>] sched_cpu_starting+0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callback_range+0x78/0x140 [0.048510] [<8108d914>]		

CVSS 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
			notify_cpu_starting +0x94/0x140 [0.048523] [<8106593c>] start_secondary+0x bc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done. ...for each but CPU 0/boot. Basic debug printks right before the mentioned line say: [0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_sta rting() calculates core-scheduling parameters only once per CPU start, and it's crucial		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to have all the parameters filled in at that moment (at least it uses cpu_smt_mask() which in fact is `&cpu_sibling_map[cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing the actual map calculation, was being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP callbacks in Linux 4.14 (see		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0] for the reference). Neither me nor my brief tests couldn't find any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now yield exactly what I expected from them: [0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.org/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef **CVE ID: CVE-2022-48845**		
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.281					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE	https://git.kernel.org/stable/c/270475d6d2410ec66e971bf181afe1958dad565e, https://git.kernel.org/stable/c/6bfc5377a210dbda2a237f16d9	O-LIN-LINU-020824/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The problem I'm addressing was discovered by the LTP test covering cve-2018-1000204. A short description of what happens follows: 1) The test case issues a command code 00 (TEST UNIT READY) via the SG_IO interface with: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_DEV and a corresponding dxferp. The peculiar thing about this is that TUR is not reading from the device. 2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808	4d1bd4f1335026, https://git.kernel.org/stable/c/7403f4118ab94be837ab9d770507537a8057bc63	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this first bounce buffer is allocated with GFP_ZERO. 3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we prepare as if the we had a DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function virtqueue_add_split() which uses DMA_FROM_DEVICE for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like		

CVSS 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
			s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we first copy back the content of the second (that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce buffer, which contains all zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized, ain't all zeros and fails. One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other participants are well behaved). Copying the content of the original buffer into the swiotlb buffer is the only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in doubt, but allow the driver to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance impact of the extra bounce. **CVE ID: CVE-2022-48853**		
Affected Version(s): From (including) 4.14.267 Up to (excluding) 4.14.273					
Integer Overflow or Wraparound	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: prevent integer overflow in	https://git.kernel.org/stable/c/138d4f739b35dfb40438a0d5d7054965763bfbe7, https://git.kernel.org/stable/c/21829376268397f9fd2c35cfa9	O-LIN-LINU-020824/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rndis_set_response() If "BufOffset" is very large the "BufOffset + 8" operation can have an integer overflow. **CVE ID: CVE-2022-48837**	135937b6aa3a1e, https://git.kernel.org/stable/c/28bc0267399f42f987916a7174e2e32f0833cc65	
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.235					
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: staging: gdm724x: fix use after free in gdm_lte_rx() The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len. **CVE ID: CVE-2022-48851**	https://git.kernel.org/stable/c/1fb9dd3787495b4deb0efe66c58306b65691a48f, https://git.kernel.org/stable/c/403e3afe241b62401de1f8629c9c6b9b3d69dbff, https://git.kernel.org/stable/c/48ecdf3e29a6e514e8196691589c7dfc6c4ac169	O-LIN-LINU-020824/349
Missing Release of Memory after Effective Lifetime	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: sctp: fix kernel-infoleak for SCTP sockets	https://git.kernel.org/stable/c/1502f15b9f29c41883a6139f2923523873282a83, https://git.kernel.org/stable/c/2d8fa3fdf4542a2174a72d92018f488d65d848c5,	O-LIN-LINU-020824/350

CVSS 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
			syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill() calls inet_diag_msg_common_fill() Make sure to clear idiag_timer/idiag_retrans/idiag_expires and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6e	https://git.kernel.org/stable/c/3fc0fd724d199e061432b66a8d85b7d48fe485f7	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline] copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h:162 [inline] simple_copy_to_iter+0xf3/0x140 net/core/datagram.c:519 __skb_datagram_iter+0x2d5/0x11b0 net/core/datagram.c:425 skb_copy_datagram_iter+0xdc/0x270 net/core/datagram.c:533 skb_copy_datagram_msg include/linux/skbuff.h:3696 [inline] netlink_recvmsg+0x669/0x1c80		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netlink/af_netlink.c:1977 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x795/0xa10 net/socket.c:2097 __do_sys_recvfrom net/socket.c:2115 [inline] __se_sys_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom+0x19d/0x210 net/socket.c:2111 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_post_alloc_hoo		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline] __kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline] __alloc_skb+0x545/0xf90 net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline] inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341		

CVSS 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_diag_rcv_msg +0x24a/0x620 netlink_rcv_skb+0x 40c/0x7e0 net/netlink/af_netl ink.c:2494 sock_diag_rcv+0x6 3/0x80 net/core/sock_diag .c:277 netlink_unicast_ker nel net/netlink/af_netl ink.c:1317 [inline] netlink_unicast+0x 1093/0x1360 net/netlink/af_netl ink.c:1343 netlink_sendmsg+0 x14d9/0x1720 net/netlink/af_netl ink.c:1919 sock_sendmsg_nos ec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline] sock_write_iter+0x 594/0x690 net/socket.c:1061		

CVSS 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
			do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851 vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00 fs/read_write.c:967 __do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120 fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000 Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not tainted 5.17.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 **CVE ID: CVE-2022-48855**		
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show When bringing down the netdevice or system shutdown, a panic can be	https://git.kernel.org/stable/c/081369ad088a76429984483b8a5f7e967a125aad, https://git.kernel.org/stable/c/3a79f380b3e10edf6caa9aac90163a5d7a282204, https://git.kernel.org/stable/c/4224cfd7fb6523f7a9d1c8bb91	O-LIN-LINU-020824/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0: Shutdown was called ... [757.937260] BUG: unable to handle kernel NULL pointer dereference at (null) [758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100 CPU: 1 COMMAND: "amsd" ... #9 [ffff89240e1a38b0	bb5df1e38eb624	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX: 0000000000001000 RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090 RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0 R13: ffff89243d874090 R14: ffff89243d874080 R15:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core] #12 [ffff89240e1a3ab8] mlx5_cmd_exec at ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8] dev_attr_show at ffffffff8f0b70e3 #20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18] kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff #25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f		

CVSS 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
			#26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START|__LINK_STATE_NOCARRIER) To prevent this scenario, we also make sure that the netdevice is present. **CVE ID: CVE-2022-48850**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in port100_send_complete Syzbot reported UAF in port100_send_complete(). The root case is in missing usb_kill_urb() calls on error handling	https://git.kernel.org/stable/c/0e721b8f2ee5e11376dd55363f9ccb539d754b8a, https://git.kernel.org/stable/c/205c4ec78e71cbf561794e6043da80e7bae6790f, https://git.kernel.org/stable/c/2b1c85f56512d49e43bc53741fce2f508cd90029	O-LIN-LINU-020824/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path of ->probe function. port100_send_complete() accesses devm allocated memory which will be freed on probe failure. We should kill this urbs before returning an error from probe function to prevent reported use-after-free Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540 by task ksoftirqd/2/26 ... Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ... Allocated by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38		

CVSS 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_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ___kasan_kmalloc mm/kasan/common.c:515 [inline] ___kasan_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524 alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320 drivers/nfc/port100.c:1502 Freed by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38		

CVSS 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_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370 ___kasan_slab_free mm/kasan/common.c:366 [inline] ___kasan_slab_free+0xff/0x140 mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501 devres_release_all+0x114/0x190 drivers/base/devres.c:530 really_probe+0x626/0xcc0 drivers/base/dd.c:670		

CVSS 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-2022-48857		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do. **CVE ID: CVE-2022-48860**	https://git.kernel.org/stable/c/1852854ee349881efb78ccdbbb237838975902e4, https://git.kernel.org/stable/c/5e7c402892e189a7bc152b125e72261154aa585d, https://git.kernel.org/stable/c/669172ce976608b25a2f76f3c65d47f042d125c9	O-LIN-LINU-020824/353
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.236					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb() which is caused by wrong	https://git.kernel.org/stable/c/35069e654bcab567ff8b9f0e68e1caf82c15dcd7, https://git.kernel.org/stable/c/5600f6986628dde888173409058847 4f54a540a8, https://git.kernel.org/stable/c/57277a8b5d881e02051ba9d7f	O-LIN-LINU-020824/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint type. There was a check for the number of endpoints, but not for the type of endpoint. Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints Fail log: usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009),	6cb3f915c229821	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ... Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320 drivers/input/input.c:629 kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593 **CVE ID: CVE-2022-48836**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug:	https://git.kernel.org/stable/c/00bdd9bf1ac6d401ad926d3d8df41b9f1399f646, https://git.kernel.org/stable/c/16b1941eac2bd499f065a6739a40ce0011a3d740, https://git.kernel.org/stable/c/2015c23610cd0	O-LIN-LINU-020824/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-syzkaller-00229-g4f12b742eb2b #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255	efadaeca4d3a8d1dae9a45aa35a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			__kasan_report mm/kasan/report.c:442 [inline]
			
			kasan_report.cold+0x83/0xdf mm/kasan/report.c:459
			
			dev_uevent+0x712/0x780 drivers/base/core.c:2320
			
			uevent_show+0x1b8/0x380 drivers/base/core.c:2391
			
			dev_attr_show+0x4b/0x90 drivers/base/core.c:2094
			
			Although the bug manifested in the driver core, the real cause was a
			race with the gadget core. dev_uevent() does:
			
			if (dev->driver)
			
			add_uevent_var(env, "DRIVER=%s", dev->driver->name);		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and between the test and the dereference of dev->driver, the gadget core sets dev->driver to NULL. The race wouldn't occur if the gadget core registered its devices on a real bus, using the standard synchronization techniques of the driver core. However, it's not necessary to make such a large change in order to fix this bug; all we need to do is make sure that udc->dev.driver is always NULL. In fact, there is no reason for udc->dev.driver ever to be set to anything, let alone to the value it currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This patch simply removes the statements in the gadget core that touch udc->dev.driver. **CVE ID: CVE-2022-48838**		
Out-of-bounds Read	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg() syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations, tpacket_rcv() is queueing skbs with garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we	https://git.kernel.org/stable/c/268dcf1f7b3193bc446ec3d14e08a240e9561e4d, https://git.kernel.org/stable/c/70b7b3c055fd4a464da8da55ff4c1f84269f9b02, https://git.kernel.org/stable/c/a055f5f2841f7522b44a2b1eccb1951b4b03d51a	O-LIN-LINU-020824/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not tainted 5.17.0-rc7-syzkaller-02396-g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0x13d/0x180 mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ___sys_recvmsg+0x2c4/0x600 net/socket.c:2632 __sys_recvmsg+0x127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae		

CVSS 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: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 0000000020000500 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000		

CVSS 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
			0 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ___sys_recvmsg+0x0/0x600 include/linux/uio.h:246 this frame has 1 object: [32, 160) 'addr' Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ========== ========== ========== ========== ====== **CVE ID: CVE-2022-48839**		
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting the following:	https://git.kernel.org/stable/c/32813321f18d5432cec1b1a6ecc964f9ea26d565, https://git.kernel.org/stable/c/56eaacb8137ba2071ce48d4e3d91979270e139a7, https://git.kernel.org/stable/c/7315f8538db009605ffba00370678142ef00ac98	O-LIN-LINU-020824/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi)) [0.048183] ------------[cut here]------------ [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc3+ #35 b7b319f24073fd9a3c2aa7ad15fb7993eec0b26f [0.048247] Stack : 817f0000 00000004 327804c8 810eb050 00000000 00000004 00000000 c314fdd1 [0.048278] 830cbd64 819c0000 81800000 817f0000 83070bf4 00000001		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			830cbd08 00000000 [0.048307] 00000000 00000000 815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34 [0.048361] 817f0000 818a3c00 817f0000 00000004 00000000 00000000 4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/0x140 [0.048424] [<8131c2a0>] dump_stack_lvl+0x60/0x80		

CVSS 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
			[0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>] warn_slowpath_fmt +0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_starting+0x198/0x240 [0.048483] [<810c6514>] sched_cpu_starting +0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callback_range+0x78/0x140 [0.048510] [<8108d914>] notify_cpu_starting +0x94/0x140 [0.048523] [<8106593c>] start_secondary+0xbc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done.		

CVSS 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
			...for each but CPU 0/boot. Basic debug printks right before the mentioned line say: [0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_starting() calculates core-scheduling parameters only once per CPU start, and it's crucial to have all the parameters filled in at that moment (at least it uses cpu_smt_mask() which in fact is `&cpu_sibling_map[cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing the actual map calculation, was		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP callbacks in Linux 4.14 (see [0] for the reference). Neither me nor my brief tests couldn't find any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now yield exactly what I expected from them:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.org/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef **CVE ID: CVE-2022-48845**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.245					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE The problem I'm addressing was discovered by the LTP test covering cve-2018-1000204. A short description of what happens follows: 1) The test case issues a command code 00 (TEST UNIT READY) via the SG_IO	https://git.kernel.org/stable/c/270475d6d2410ec66e971bf181afe1958dad565e, https://git.kernel.org/stable/c/6bfc5377a210dbda2a237f16d94d1bd4f1335026, https://git.kernel.org/stable/c/7403f4118ab94be837ab9d770507537a8057bc63	O-LIN-LINU-020824/358

CVSS 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: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_ DEV and a corresponding dxferp. The peculiar thing about this is that TUR is not reading from the device. 2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808 ("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this first bounce buffer is allocated with GFP_ZERO. 3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we prepare as if the we had a		

CVSS 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
			DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function virtqueue_add_split() which uses DMA_FROM_DEVICE for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we first copy back the content of the second (that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce buffer, which contains all		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized, ain't all zeros and fails. One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all other participants are well behaved). Copying the content of the original buffer into the swiotlb buffer is the only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in doubt, but allow the driver		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance impact of the extra bounce. **CVE ID: CVE-2022-48853**		
Affected Version(s): From (including) 4.18 Up to (excluding) 4.19.235					
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gianfar: ethtool: Fix refcount leak in gfar_get_ts_info The of_find_compatible_node() function returns a node pointer with refcount incremented, We should use of_node_put() on it when done Add the missing of_node_put() to release the refcount. **CVE ID: CVE-2022-48856**	https://git.kernel.org/stable/c/0e1b9a2078e07fb1e6e91bf8badfd89ecab1e848, https://git.kernel.org/stable/c/21044e679ed535345042d2023f7df0ca8e897e2a, https://git.kernel.org/stable/c/2ac5b58e645c66932438bb021cb5b52097ce70b0	O-LIN-LINU-020824/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.19 Up to (excluding) 5.10.221					
Allocation of Resources Without Limits or Throttling	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params	https://git.kernel.org/stable/c/1095b8efbb13a6a5fa583ed373ee1ccab29da2d0, https://git.kernel.org/stable/c/14e51ea78b4ccacb7acb1346b9241bb790a2054c, https://git.kernel.org/stable/c/1d3e3b3aa2cbe9bc7db9a7f8673a9fa6d2990d54	O-LIN-LINU-020824/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			struct with valid fields. So, warning is only triggered when there is a problem with memory allocation. Thus, there is no sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650		

CVSS 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/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_live+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline]		

CVSS 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
			__x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Found by Linux Verification Center (linuxtesting.org) with syzkaller. **CVE ID: CVE-2024-42082**		
Affected Version(s): From (including) 4.19.230 Up to (excluding) 4.19.236					
Integer Overflow or Wraparound	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: prevent integer overflow in rndis_set_response() If "BufOffset" is very large the "BufOffset + 8" operation can have an integer overflow. **CVE ID: CVE-2022-48837**	https://git.kernel.org/stable/c/138d4f739b35dfb40438a0d5d7054965763bfbe7, https://git.kernel.org/stable/c/21829376268397f9fd2c35cfa9135937b6aa3a1e, https://git.kernel.org/stable/c/28bc0267399f42f987916a7174e2e32f0833cc65	O-LIN-LINU-020824/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.185					
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: staging: gdm724x: fix use after free in gdm_lte_rx() The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len. **CVE ID: CVE-2022-48851**	https://git.kernel.org/stable/c/1fb9dd3787495b4deb0efe66c58306b65691a48f, https://git.kernel.org/stable/c/403e3afe241b62401de1f8629c9c6b9b3d69dbff, https://git.kernel.org/stable/c/48ecdf3e29a6e514e8196691589c7dfc6c4ac169	O-LIN-LINU-020824/362
Missing Release of Memory after Effective Lifetime	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: sctp: fix kernel-infoleak for SCTP sockets syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill() calls inet_diag_msg_common_fill()	https://git.kernel.org/stable/c/1502f15b9f29c41883a6139f2923523873282a83, https://git.kernel.org/stable/c/2d8fa3fdf4542a2174a72d92018f488d65d848c5, https://git.kernel.org/stable/c/3fc0fd724d199e061432b66a8d85b7d48fe485f7	O-LIN-LINU-020824/363

CVSS 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
			Make sure to clear idiag_timer/idiag_retrans/idiag_expires and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline] copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6e		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h :162 [inline] simple_copy_to_iter +0xf3/0x140 net/core/datagram .c:519 __skb_datagram_ite r+0x2d5/0x11b0 net/core/datagram .c:425 skb_copy_datagram _iter+0xdc/0x270 net/core/datagram .c:533 skb_copy_datagram _msg include/linux/skbu ff.h:3696 [inline] netlink_recvmsg+0 x669/0x1c80 net/netlink/af_netl ink.c:1977 sock_recvmsg_nose c net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x 795/0xa10 net/socket.c:2097		

CVSS 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
			__do_sys_recvfrom net/socket.c:2115 [inline] __se_sys_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom +0x19d/0x210 net/socket.c:2111 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_post_alloc_hook mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline] __kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__alloc_skb+0x545/0xf90 net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline] inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341 sock_diag_rcv_msg+0x24a/0x620 netlink_rcv_skb+0x40c/0x7e0 net/netlink/af_netlink.c:2494 sock_diag_rcv+0x63/0x80 net/core/sock_diag.c:277		

CVSS 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
			netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline] netlink_unicast+0x1093/0x1360 net/netlink/af_netlink.c:1343 netlink_sendmsg+0x14d9/0x1720 net/netlink/af_netlink.c:1919 sock_sendmsg_nosec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline] sock_write_iter+0x594/0x690 net/socket.c:1061 do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851 vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fs/read_write.c:967 __do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120 fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000 Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tainted 5.17.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 **CVE ID: CVE-2022-48855**		
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show When bringing down the netdevice or system shutdown, a panic can be triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0:	https://git.kernel.org/stable/c/081369ad088a76429984483b8a5f7e967a125aad, https://git.kernel.org/stable/c/3a79f380b3e10edf6caa9aac90163a5d7a282204, https://git.kernel.org/stable/c/4224cfd7fb6523f7a9d1c8bb91bb5df1e38eb624	O-LIN-LINU-020824/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Shutdown was called ... [757.937260] BUG: unable to handle kernel NULL pointer dereference at (null) [758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100 CPU: 1 COMMAND: "amsd" ... #9 [ffff89240e1a38b0] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000001000 RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090 RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0 R13: ffff89243d874090 R14: ffff89243d874080 R15: 0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#12 [ffff89240e1a3ab8] mlx5_cmd_exec at ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08] mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			] dev_attr_show at ffffffff8f0b70e3 #20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18] kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff #25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f #26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START| __LINK_STATE_NOCARRIER)		

CVSS 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
			To prevent this scenario, we also make sure that the netdevice is present. **CVE ID: CVE-2022-48850**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gianfar: ethtool: Fix refcount leak in gfar_get_ts_info The of_find_compatible_node() function returns a node pointer with refcount incremented, We should use of_node_put() on it when done Add the missing of_node_put() to release the refcount. **CVE ID: CVE-2022-48856**	https://git.kernel.org/stable/c/0e1b9a2078e07fb1e6e91bf8badfd89ecab1e848, https://git.kernel.org/stable/c/21044e679ed535345042d2023f7df0ca8e897e2a, https://git.kernel.org/stable/c/2ac5b58e645c66932438bb021cb5b52097ce70b0	O-LIN-LINU-020824/365
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in	https://git.kernel.org/stable/c/0e721b8f2ee5e11376dd55363f9ccb539d754b8a, https://git.kernel.org/stable/c/205c4ec78e71c	O-LIN-LINU-020824/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			port100_send_complete Syzbot reported UAF in port100_send_complete(). The root case is in missing usb_kill_urb() calls on error handling path of ->probe function. port100_send_complete() accesses devm allocated memory which will be freed on probe failure. We should kill this urbs before returning an error from probe function to prevent reported use-after-free Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540	bf561794e6043da80e7bae6790f, https://git.kernel.org/stable/c/2b1c85f56512d49e43bc53741fce2f508cd90029	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by task ksoftirqd/2/26 ... Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ...		

CVSS 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
			Allocated by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ___kasan_kmalloc mm/kasan/common.c:515 [inline] ___kasan_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524 alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320		

CVSS 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
			drivers/nfc/port100.c:1502 Freed by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370 ___kasan_slab_free mm/kasan/common.c:366 [inline] ___kasan_slab_free+0xff/0x140 mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devres_release_all+0x114/0x190 drivers/base/devres.c:530 really_probe+0x626/0xcc0 drivers/base/dd.c:670 **CVE ID: CVE-2022-48857**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do. **CVE ID: CVE-2022-48860**	https://git.kernel.org/stable/c/1852854ee349881efb78ccdbbb237838975902e4, https://git.kernel.org/stable/c/5e7c402892e189a7bc152b125e72261154aa585d, https://git.kernel.org/stable/c/669172ce976608b25a2f76f3c65d47f042d125c9	O-LIN-LINU-020824/367
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.186					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/32813321f18d5432cec1b1a6ecc964f9ea26d56	O-LIN-LINU-020824/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting the following: [0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi)) [0.048183] ------------[cut here]------------ [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc3+ #35 b7b319f24073fd9a3c2aa7ad15fb7993eec0b26f	5, https://git.kernel.org/stable/c/56eaacb8137ba2071ce48d4e3d91979270e139a7, https://git.kernel.org/stable/c/7315f8538db009605ffba00370678142ef00ac98	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.048247] Stack : 817f0000 00000004 327804c8 810eb050 00000000 00000004 00000000 c314fdd1 [0.048278] 830cbd64 819c0000 81800000 817f0000 83070bf4 00000001 830cbd08 00000000 [0.048307] 00000000 00000000 815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34 [0.048361] 817f0000 818a3c00 817f0000 00000004 00000000 00000000		

CVSS 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
			4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/ 0x140 [0.048424] [<8131c2a0>] dump_stack_lvl+0x 60/0x80 [0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>] warn_slowpath_fmt +0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_sta rting+0x198/0x24 0 [0.048483] [<810c6514>] sched_cpu_starting +0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callb ack_range+0x78/0 x140 [0.048510] [<8108d914>] notify_cpu_starting +0x94/0x140 [0.048523] [<8106593c>]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			start_secondary+0xbc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done. ...for each but CPU 0/boot. Basic debug printks right before the mentioned line say: [0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_starting() calculates core-scheduling parameters only once per CPU start, and it's crucial to have all the parameters filled in at that moment (at least it		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uses cpu_smt_mask() which in fact is `&cpu_sibling_map[ cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing the actual map calculation, was being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP callbacks in Linux 4.14 (see [0] for the reference). Neither me nor my brief tests couldn't find		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now yield exactly what I expected from them: [0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.org/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef **CVE ID: CVE-2022-48845**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.187					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb()	https://git.kernel.org/stable/c/35069e654bcab567ff8b9f0e68e1caf82c15dcd7, https://git.kernel.org/stable/c/5600f6986628dde8881734090588474f54a540a8, https://git.kernel.org/stable/c/57277a8b5d881e02051ba9d7f	O-LIN-LINU-020824/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which is caused by wrong endpoint type. There was a check for the number of endpoints, but not for the type of endpoint. Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints Fail log: usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC	6cb3f915c229821	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ... Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320 drivers/input/input.c:629 kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593 **CVE ID: CVE-2022-48836**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug:	https://git.kernel.org/stable/c/00bdd9bf1ac6d401ad926d3d8df41b9f1399f646, https://git.kernel.org/stable/c/16b1941eac2bd499f065a6739a40ce0011a3d740, https://git.kernel.org/stable/c/2015c23610cd0	O-LIN-LINU-020824/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-syzkaller-00229-g4f12b742eb2b #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255	efadaeca4d3a8d1dae9a45aa35a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			__kasan_report mm/kasan/report.c:442 [inline]
			
			kasan_report.cold+0x83/0xdf mm/kasan/report.c:459
			
			dev_uevent+0x712/0x780 drivers/base/core.c:2320
			
			uevent_show+0x1b8/0x380 drivers/base/core.c:2391
			
			dev_attr_show+0x4b/0x90 drivers/base/core.c:2094
			
			Although the bug manifested in the driver core, the real cause was a
			race with the gadget core. dev_uevent() does:
			
			if (dev->driver)
			
			add_uevent_var(env, "DRIVER=%s", dev->driver->name);		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and between the test and the dereference of dev->driver, the gadget core sets dev->driver to NULL. The race wouldn't occur if the gadget core registered its devices on a real bus, using the standard synchronization techniques of the driver core. However, it's not necessary to make such a large change in order to fix this bug; all we need to do is make sure that udc->dev.driver is always NULL. In fact, there is no reason for udc->dev.driver ever to be set to anything, let alone to the value it currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This patch simply removes the statements in the gadget core that touch udc->dev.driver. **CVE ID: CVE-2022-48838**		
Out-of-bounds Read	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg() syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations, tpacket_rcv() is queueing skbs with garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we	https://git.kernel.org/stable/c/268dcf1f7b3193bc446ec3d14e08a240e9561e4d, https://git.kernel.org/stable/c/70b7b3c055fd4a464da8da55ff4c1f84269f9b02, https://git.kernel.org/stable/c/a055f5f2841f7522b44a2b1eccb1951b4b03d51a	O-LIN-LINU-020824/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not tainted 5.17.0-rc7-syzkaller-02396-g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0x13d/0x180 mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ___sys_recvmsg+0x2c4/0x600 net/socket.c:2632 __sys_recvmsg+0x127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae		

CVSS 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: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 0000000020000500 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ___sys_recvmsg+0x0/0x600 include/linux/uio.h:246 this frame has 1 object: [32, 160) 'addr' Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ========== ========== ========== ========== ====== **CVE ID: CVE-2022-48839**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.189					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE The problem I'm addressing was discovered by the LTP test covering cve-2018-1000204.	https://git.kernel.org/stable/c/270475d6d2410ec66e971bf181afe1958dad565e, https://git.kernel.org/stable/c/6bfc5377a210dbda2a237f16d94d1bd4f1335026, https://git.kernel.org/stable/c/7403f4118ab94be837ab9d770507537a8057bc63	O-LIN-LINU-020824/372

CVSS 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
			A short description of what happens follows: 1) The test case issues a command code 00 (TEST UNIT READY) via the SG_IO interface with: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_ DEV and a corresponding dxferp. The peculiar thing about this is that TUR is not reading from the device. 2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808 ("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this first bounce buffer is allocated with GFP_ZERO.		

CVSS 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
			3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we prepare as if the we had a DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function virtqueue_add_split() which uses DMA_FROM_DEVICE for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we first copy back the content of the second		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce buffer, which contains all zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized, ain't all zeros and fails. One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all other participants are well behaved). Copying the content of the original buffer into the swiotlb buffer is		

CVSS 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 only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in doubt, but allow the driver to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance impact of the extra bounce. **CVE ID: CVE-2022-48853**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.279					
Missing Release of Memory after Effective Lifetime	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either	https://git.kernel.org/stable/c/23752737c6a618e994f9a310ec2568881a6b49c4, https://git.kernel.org/stable/c/40188a25a9847dbeb7ec67517174a835a677752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b5153848bfa1c2980f	O-LIN-LINU-020824/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers. **CVE ID: CVE-2024-42070**		
Affected Version(s): From (including) 4.4 Up to (excluding) 4.9.308					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb() which is caused by wrong endpoint type. There was a check for the number of endpoints, but not for the type of endpoint.	https://git.kernel.org/stable/c/35069e654bcab567ff8b9f0e68e1caf82c15dcd7, https://git.kernel.org/stable/c/5600f6986628dde888173409058847 4f54a540a8, https://git.kernel.org/stable/c/57277a8b5d881e02051ba9d7f6cb3f915c229821	O-LIN-LINU-020824/374

CVSS 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
			Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints Fail log: usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ...		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320 drivers/input/input.c:629 kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593 **CVE ID: CVE-2022-48836**		
Affected Version(s): From (including) 4.7 Up to (excluding) 4.9.307					
Missing Release of Memory after Effective Lifetime	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: sctp: fix kernel-infoleak for SCTP sockets syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill()	https://git.kernel.org/stable/c/1502f15b9f29c41883a6139f2923523873282a83, https://git.kernel.org/stable/c/2d8fa3fdf4542a2174a72d92018f488d65d848c5, https://git.kernel.org/stable/c/3fc0fd724d199e061432b66a8d85b7d48fe485f7	O-LIN-LINU-020824/375

CVSS 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
			calls inet_diag_msg_common_fill() Make sure to clear idiag_timer/idiag_retrans/idiag_expires and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline]		

CVSS 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
			copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h:162 [inline] simple_copy_to_iter+0xf3/0x140 net/core/datagram.c:519 __skb_datagram_iter+0x2d5/0x11b0 net/core/datagram.c:425 skb_copy_datagram_iter+0xdc/0x270 net/core/datagram.c:533 skb_copy_datagram_msg include/linux/skbuff.h:3696 [inline] netlink_recvmsg+0x669/0x1c80 net/netlink/af_netlink.c:1977 sock_recvmsg_nosec net/socket.c:948 [inline]		

CVSS 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_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x795/0xa10 net/socket.c:2097 __do_sys_recvfrom net/socket.c:2115 [inline] __se_sys_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom+0x19d/0x210 net/socket.c:2111 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_post_alloc_hook mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline]		

CVSS 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
			__kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline] __alloc_skb+0x545/0xf90 net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline] inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341 sock_diag_rcv_msg+0x24a/0x620 netlink_rcv_skb+0x40c/0x7e0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netlink/af_netlink.c:2494 sock_diag_rcv+0x63/0x80 net/core/sock_diag.c:277 netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline] netlink_unicast+0x1093/0x1360 net/netlink/af_netlink.c:1343 netlink_sendmsg+0x14d9/0x1720 net/netlink/af_netlink.c:1919 sock_sendmsg_nosec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline] sock_write_iter+0x594/0x690 net/socket.c:1061 do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851		

CVSS 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
			vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00 fs/read_write.c:967 __do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120 fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000		

CVSS 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
			Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not tainted 5.17.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 **CVE ID: CVE-2022-48855**		
Affected Version(s): From (including) 4.7 Up to (excluding) 5.10.221					
N/A	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does	https://git.kernel.org/stable/c/320273b5649bbcee87f9e65343077189699d2a7a, https://git.kernel.org/stable/c/331d1079d58206ff7dc5518185f800b412f89bc6, https://git.kernel.org/stable/c/9ea2d1c6789722d58ec191f14f9a02518d55b6b4	O-LIN-LINU-020824/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not take into account that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OCFS2 aborts in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 filesystem. To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2] #4 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f		

CVSS 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
			#13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba **CVE ID: CVE-2024-42077**		
Affected Version(s): From (including) 4.8 Up to (excluding) 5.10.106					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tipc: fix kernel panic when enabling bearer	https://git.kernel.org/stable/c/2de76d37d4a6dca9b96ea51da24d4290e6cfa1a5, https://git.kernel.org/stable/c/be4977b847f5d	O-LIN-LINU-020824/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When enabling a bearer on a node, a kernel panic is observed: [4.498085] RIP: 0010:tipc_mon_prep+0x4e/0x130 [tipc] ... [4.520030] Call Trace: [4.520689] <IRQ> [4.521236] tipc_link_build_proto_msg+0x375/0x750 [tipc] [4.522654] tipc_link_build_state_msg+0x48/0xc0 [tipc] [4.524034] __tipc_node_link_up+0xd7/0x290 [tipc] [4.525292] tipc_rcv+0x5da/0x730 [tipc] [4.526346] ? __netif_receive_skb_core+0xb7/0xfc0 [4.527601] tipc_l2_rcv_msg+0x5e/0x90 [tipc] [4.528737] __netif_receive_skb_list_core+0x20b/0x260	5cedb64d50eaaf2218c3a55a3a3, https://git.kernel.org/stable/c/f4f59fdbc748805b08c13dae14c01f0518c77c94	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4.530068] netif_receive_skb_list_internal+0x1bf/0x2e0 [4.531450] ? dev_gro_receive+0x4c2/0x680 [4.532512] napi_complete_done+0x6f/0x180 [4.533570] virtnet_poll+0x29c/0x42e [virtio_net] ... The node in question is receiving activate messages in another thread after changing bearer status to allow message sending/ receiving in current thread: thread 1 | thread 2 -------- | -------- | tipc_enable_bearer() | test_and_set_bit_lock() |		

CVSS 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

			tipc_bearer_xmit_skb() |
			|
			tipc_l2_rcv_msg()
			|
			tipc_rcv()
			|
			__tipc_node_link_up()
			|
			tipc_link_build_state_msg()
			|
			tipc_link_build_proto_msg()
			|
			tipc_mon_prep()
			|
			{
			|
			...
			|
			// null-pointer dereference
			|
			u16 gen = mon->dom_gen;
			|
			...
			|
			}
			// Not being executed yet |
			tipc_mon_create()
			|
			{ |
			... |		

CVSS 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
			// allocate | mon = kzalloc(); | ... | } | Monitoring pointer in thread 2 is dereferenced before monitoring data is allocated in thread 1. This causes kernel panic. This commit fixes it by allocating the monitoring data before enabling the bearer to receive messages. **CVE ID: CVE-2022-48865**		
Affected Version(s): From (including) 4.9.302 Up to (excluding) 4.9.308					
Integer Overflow or Wraparound	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: prevent integer overflow in rndis_set_response() If "BufOffset" is very large the "BufOffset + 8"	https://git.kernel.org/stable/c/138d4f739b35dfb40438a0d5d7054965763bfbe7, https://git.kernel.org/stable/c/21829376268397f9fd2c35cfa9135937b6aa3a1e, https://git.kernel.org/stable/c/28bc0267399f4	O-LIN-LINU-020824/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation can have an integer overflow. **CVE ID: CVE-2022-48837**	2f987916a7174e2e32f0833cc65	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.10.108					
Release of Invalid Pointer or Reference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Page fault in reply q processing A page fault was encountered in mpt3sas on a LUN reset error path: [145.763216] mpt3sas_cm1: Task abort tm failed: handle(0x0002),timeout(30) tr_method(0x0) smid(3) msix_index(0) [145.778932] scsi 1:0:0:0: task abort: FAILED scmd(0x0000000024ba29a2) [145.817307] scsi 1:0:0:0: attempting device reset! scmd(0x0000000024ba29a2) [145.827253] scsi 1:0:0:0: [sg1] tag#2	https://git.kernel.org/stable/c/0cd2dd4bcf4abc812148c4943f966a3c8dccb00f, https://git.kernel.org/stable/c/3916e33b917581e2b2086e856c291cb86ea98a05, https://git.kernel.org/stable/c/69ad4ef868c1fc7609daa235dfa46d28ba7a3ba3	O-LIN-LINU-020824/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CDB: Receive Diagnostic 1c 01 01 ff fc 00 [145.837617] scsi target1:0:0: handle(0x0002), sas_address(0x500605b0000272b9), phy(0) [145.848598] scsi target1:0:0: enclosure logical id(0x500605b0000272b8), slot(0) [149.858378] mpt3sas_cm1: Poll ReplyDescriptor queues for completion of smid(0), task_type(0x05), handle(0x0002) [149.875202] BUG: unable to handle page fault for address: 00000007fffc445d [149.885617] #PF: supervisor read access in kernel mode [149.894346] #PF: error_code(0x0000) - not-present page [149.903123] PGD 0 P4D 0 [149.909387] Oops: 0000 [#1] PREEMPT SMP NOPTI		

CVSS 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
			[149.917417] CPU: 24 PID: 3512 Comm: scsi_eh_1 Kdump: loaded Tainted: G S O 5.10.89-altav-1 #1 [149.934327] Hardware name: DDN 200NVX2 /200NVX2-MB , BIOS ATHG2.2.02.01 09/10/2021 [149.951871] RIP: 0010:_base_process_reply_queue+0x4b/0x900 [mpt3sas] [149.961889] Code: 0f 84 22 02 00 00 8d 48 01 49 89 fd 48 8d 57 38 f0 0f b1 4f 38 0f 85 d8 01 00 00 49 8b 45 10 45 31 e4 41 8b 55 0c 48 8d 1c d0 <0f> b6 03 83 e0 0f 3c 0f 0f 85 a2 00 00 00 e9 e6 01 00 00 0f b7 ee [149.991952] RSP: 0018:ffffc9000f1ebcb8 EFLAGS: 00010246 [150.000937] RAX: 0000000000000055 RBX: 00000007fffc445d RCX: 000000002548f071		

CVSS 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
			[150.011841] RDX: 00000000ffff8881 RSI: 0000000000000001 RDI: ffff888125ed50d8 [150.022670] RBP: 0000000000000000 R08: 0000000000000000 R09: c0000000ffff7fff [150.033445] R10: ffffc9000f1ebb68 R11: ffffc9000f1ebb60 R12: 0000000000000000 [150.044204] R13: ffff888125ed50d8 R14: 0000000000000080 R15: 34cdc00034cdea80 [150.054963] FS: 0000000000000000(0000) GS:ffff88dfaf200000(0000) knlGS:0000000000000000 [150.066715] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [150.076078] CR2: 00000007fffc445d CR3:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			000000012448a006 CR4: 0000000000770ee0 [150.086887] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [150.097670] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [150.108323] PKRU: 55555554 [150.114690] Call Trace: [150.120497] ? printk+0x48/0x4a [150.127049] mpt3sas_scsih_issue_tm.cold.114+0x2e/0x2b3 [mpt3sas] [150.136453] mpt3sas_scsih_issue_locked_tm+0x86/0xb0 [mpt3sas] [150.145759] scsih_dev_reset+0xea/0x300 [mpt3sas] [150.153891] scsi_eh_ready_devs		

CVSS 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
			+0x541/0x9e0 [scsi_mod] [150.162206] ? __scsi_host_match+0x20/0x20 [scsi_mod] [150.170406] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.178925] ? blk_mq_tagset_busy_iter+0x45/0x60 [150.186638] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.195087] scsi_error_handler+0x3a5/0x4a0 [scsi_mod] [150.203206] ? __schedule+0x1e9/0x610 [150.209783] ? scsi_eh_get_sense+0x210/0x210 [scsi_mod] [150.217924] kthread+0x12e/0x150 [150.224041] ? kthread_worker_fn+0x130/0x130 [150.231206] ret_from_fork+0x1f/0x30 This is caused by mpt3sas_base_sync		

CVSS 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
			_reply_irqs() using an invalid reply_q pointer outside of the list_for_each_entry() loop. At the end of the full list traversal the pointer is invalid. Move the _base_process_reply_queue() call inside of the loop. **CVE ID: CVE-2022-48835**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.15.29					
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: marvell: prestera: Add missing of_node_put() in prestera_switch_set_base_mac_addr This node pointer is returned by of_find_compatible_node() with refcount incremented. Calling of_node_put() to aovid the refcount leak.	https://git.kernel.org/stable/c/4cc66bf17220ff9631f9fa99b02a872e0ad5a08b, https://git.kernel.org/stable/c/b7c2fd1d126329340639adfb8dd2938fe4b65df7, https://git.kernel.org/stable/c/c9ffa3e2bc451816ce0295e40063514fabf2bd36	O-LIN-LINU-020824/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48859		
Affected Version(s): From (including) 5.10.101 Up to (excluding) 5.10.108					
Integer Overflow or Wraparound	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: prevent integer overflow in rndis_set_response() If "BufOffset" is very large the "BufOffset + 8" operation can have an integer overflow. **CVE ID: CVE-2022-48837**	https://git.kernel.org/stable/c/138d4f739b35dfb40438a0d5d7054965763bfbe7, https://git.kernel.org/stable/c/21829376268397f9fd2c35cfa9135937b6aa3a1e, https://git.kernel.org/stable/c/28bc0267399f42f987916a7174e2e32f0833cc65	O-LIN-LINU-020824/381
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.162					
Missing Release of Memory after Effective Lifetime	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however,	https://git.kernel.org/stable/c/23752737c6a618e994f9a310ec2568881a6b49c4, https://git.kernel.org/stable/c/40188a25a9847dbeb7ec67517174a835a677752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b515	O-LIN-LINU-020824/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers. **CVE ID: CVE-2024-42070**	3848bfa1c2980f	
Use of Uninitialized Resource	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak	https://git.kernel.org/stable/c/4c5dc3927e17489c1cae6f48c0d5e4acb4cae01f, https://git.kernel.org/stable/c/5e4ed38eb17eaca42de57d500cc0f9668d2b6abf, https://git.kernel.org/stable/c/a2a0ebff7fdeb2f66e29335adf64b9e457300dd4	O-LIN-LINU-020824/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_t		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			o_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c4/0x340 net/socket.c:1068 ___sys_recvmsg+0x18a/0x620 net/socket.c:2803 __sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0		

CVSS 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
			arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_ps		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline]		

CVSS 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
			__do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg +0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b /0x3b50 arch/x86/include/ generated/asm/sy scalls_64.h:47 do_syscall_x64 arch/x86/entry/co mmon.c:52 [inline] do_syscall_64+0xcf /0x1e0 arch/x86/entry/co mmon.c:83 entry_SYSCALL_64_ after_hwframe+0x 77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c 0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 **CVE ID: CVE-2024-42076**		
N/A	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can	https://git.kernel.org/stable/c/320273b5649bbcee87f9e65343077189699d2a7a, https://git.kernel.org/stable/c/331d1079d58206ff7dc5518185f800b412f89bc6, https://git.kernel.org/stable/c/9ea2d1c6789722d58ec191f14f9a02518d55b6b4	O-LIN-LINU-020824/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain arbitrary number of extents. Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by one of our customers on a heavily fragmented OCFS2 filesystem. To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2]		

CVSS 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 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_		

CVSS 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
			write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba **CVE ID: CVE-2024-42077**		
Allocation of Resources Without Limits or Throttling	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model().	https://git.kernel.org/stable/c/1095b8efbb13a6a5fa583ed373ee1ccab29da2d0, https://git.kernel.org/stable/c/14e51ea78b4ccacb7acb1346b9241bb790a2054c, https://git.kernel.org/stable/c/1d3e3b3aa2cbe9bc7db9a7f867	O-LIN-LINU-020824/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation. Thus, there is no sense in using WARN() to handle this error and it can be safely removed.	3a9fa6d2990d54	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_li		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ve+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Found by Linux Verification Center		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(linuxtesting.org) with syzkaller. **CVE ID: CVE-2024-42082**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.163					
N/A	30-Jul-2024	4.1	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accomplish this by using kfree_sensitive for buffers that previously held the private key. **CVE ID: CVE-2024-42229**	https://git.kernel.org/stable/c/23e4099bdc3c8381992f9eb975c7919 6d6755210, https://git.kernel.org/stable/c/28c8d274848feba552e95c5c2a7e3cfe8f15c534, https://git.kernel.org/stable/c/71dd428615375e36523f4d4f7685ddd54113646d	O-LIN-LINU-020824/386
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.29					
Out-of-bounds Write	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1b09f28f70a5046acd64138075ae3f095238b045, https://git.kern	O-LIN-LINU-020824/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			watch_queue: Fix filter limit check
			
			In watch_queue_set_filter(), there are a couple of places where we check
			that the filter type value does not exceed what the type_filter bitmap
			can hold. One place calculates the number of bits by:
			
			if (tf[i].type >= sizeof(wfilter->type_filter) * 8)
			
			which is fine, but the second does:
			
			if (tf[i].type >= sizeof(wfilter->type_filter) * BITS_PER_LONG)
			
			which is not. This can lead to a couple of out-of-bounds writes due to
			a too-large type:
			
			(1) __set_bit() on wfilter->type_filter
			(2) Writing more elements in wfilter-
				el.org/stable/c/648895da69ced90ca770fd941c3d9479a9d72c16, https://git.kernel.org/stable/c/b36588ebbcef74583824c08352e75838d6fb4ff2	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>filters[] than we allocated. Fix this by just using the proper WATCH_TYPE__NR instead, which is the number of types we actually know about. The bug may cause an oops looking something like: BUG: KASAN: slab-out-of-bounds in watch_queue_set_filter+0x659/0x740 Write of size 4 at addr ffff88800d2c66bc by task watch_queue_oob/611 ... Call Trace: <TASK> dump_stack_lvl+0x45/0x59 print_address_description.constprop.0+0x1f/0x150 ...		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_report.cold+0x7f/0x11b ... watch_queue_set_filter+0x659/0x740 ... __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae Allocated by task 611: kasan_save_stack+0x1e/0x40 __kasan_kmalloc+0x81/0xa0 watch_queue_set_filter+0x23a/0x740 __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after_hwframe+0x44/0xae The buggy address belongs to the object at ffff88800d2c66a0 which belongs to the cache kmalloc-32 of size 32 The buggy address is located 28 bytes inside of 32-byte region [ffff88800d2c66a0, ffff88800d2c66c0) **CVE ID: CVE-2022-48847**		
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: staging: gdm724x: fix use after free in gdm_lte_rx() The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len. **CVE ID: CVE-2022-48851**	https://git.kernel.org/stable/c/1fb9dd3787495b4deb0efe66c58306b65691a48f, https://git.kernel.org/stable/c/403e3afe241b62401de1f8629c9c6b9b3d69dbff, https://git.kernel.org/stable/c/48ecdf3e29a6e514e8196691589c7dfc6c4ac169	O-LIN-LINU-020824/388
Missing Release of Memory after	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1502f15b9f29c41883a6139f2923523873282a	O-LIN-LINU-020824/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			sctp: fix kernel-infoleak for SCTP sockets syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill() calls inet_diag_msg_common_fill() Make sure to clear idiag_timer/idiag_retrans/idiag_expires and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout	83, https://git.kernel.org/stable/c/2d8fa3fdf4542a2174a72d92018f488d65d848c5, https://git.kernel.org/stable/c/3fc0fd724d199e061432b66a8d85b7d48fe485f7	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline] copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h:162 [inline] simple_copy_to_iter+0xf3/0x140 net/core/datagram.c:519 __skb_datagram_iter+0x2d5/0x11b0 net/core/datagram.c:425 skb_copy_datagram_iter+0xdc/0x270 net/core/datagram.c:533 skb_copy_datagram_msg		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/skbuff.h:3696 [inline] netlink_recvmsg+0x669/0x1c80 net/netlink/af_netlink.c:1977 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x795/0xa10 net/socket.c:2097 __do_sys_recvfrom net/socket.c:2115 [inline] __se_sys_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom+0x19d/0x210 net/socket.c:2111 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Uninit was created at: slab_post_alloc_hook mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline] __kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline] __alloc_skb+0x545/0xf90 net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline]		

CVSS 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
			inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341 sock_diag_rcv_msg+0x24a/0x620 netlink_rcv_skb+0x40c/0x7e0 net/netlink/af_netlink.c:2494 sock_diag_rcv+0x63/0x80 net/core/sock_diag.c:277 netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline] netlink_unicast+0x1093/0x1360 net/netlink/af_netlink.c:1343 netlink_sendmsg+0x14d9/0x1720 net/netlink/af_netlink.c:1919 sock_sendmsg_nosec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline]		

CVSS 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_write_iter+0x594/0x690 net/socket.c:1061 do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851 vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00 fs/read_write.c:967 __do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120 fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_		

CVSS 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
			after_hwframe+0x44/0xae Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000 Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not tainted 5.17.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 **CVE ID: CVE-2022-48855**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Jul-2024	7	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix a race on command flush flow Fix a refcount use after free warning	https://git.kernel.org/stable/c/0401bfb27a91d7bdd74b1635c1aae57cbb128da6, https://git.kernel.org/stable/c/063bd355595428750803d8736a9bb7c8db67d42d, https://git.kernel.org/stable/c/	O-LIN-LINU-020824/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a race on command entry. Such race occurs when one of the commands releases its last refcount and frees its index and entry while another process running command flush flow takes refcount to this command entry. The process which handles commands flush may see this command as needed to be flushed if the other process released its refcount but didn't release the index yet. Fix it by adding the needed spin lock. It fixes the following warning trace: refcount_t: addition on 0; use-after-free. WARNING: CPU: 11 PID: 540311 at lib/refcount.c:25 refcount_warn_saturate+0x80/0xe0 ... RIP: 0010:refcount_war	1a4017926eeea56c7540cc41b42106746ee8a0ee	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n_saturate+0x80/0xe0 ... Call Trace: <TASK> mlx5_cmd_trigger_completions+0x293/0x340 [mlx5_core] mlx5_cmd_flush+0x3a/0xf0 [mlx5_core] enter_error_state+0x44/0x80 [mlx5_core] mlx5_fw_fatal_reporter_err_work+0x37/0xe0 [mlx5_core] process_one_work+0x1be/0x390 worker_thread+0x4d/0x3d0 ? rescuer_thread+0x350/0x350 kthread+0x141/0x160 ? set_kthread_struct+0x40/0x40		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ret_from_fork+0x1f/0x30 </TASK> **CVE ID: CVE-2022-48858**		
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show When bringing down the netdevice or system shutdown, a panic can be triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0: Shutdown was called ...	https://git.kernel.org/stable/c/081369ad088a76429984483b8a5f7e967a125aad, https://git.kernel.org/stable/c/3a79f380b3e10edf6caa9aac90163a5d7a282204, https://git.kernel.org/stable/c/4224cfd7fb6523f7a9d1c8bb91bb5df1e38eb624	O-LIN-LINU-020824/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[757.937260] BUG: unable to handle kernel NULL pointer dereference at (null) [758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100 CPU: 1 COMMAND: "amsd" ... #9 [ffff89240e1a38b0] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX: 0000000000001000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090 RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0 R13: ffff89243d874090 R14: ffff89243d874080 R15: 0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core] #12 [ffff89240e1a3ab8] mlx5_cmd_exec at		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08] mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8] dev_attr_show at ffffffff8f0b70e3		

CVSS 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
			#20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18] kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff #25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f #26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START| __LINK_STATE_NOCARRIER) To prevent this scenario, we also		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make sure that the netdevice is present. **CVE ID: CVE-2022-48850**		
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE The problem I'm addressing was discovered by the LTP test covering cve-2018-1000204. A short description of what happens follows: 1) The test case issues a command code 00 (TEST UNIT READY) via the SG_IO interface with: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_DEV and a corresponding dxferp. The peculiar thing	https://git.kernel.org/stable/c/270475d6d2410ec66e971bf181afe1958dad565e, https://git.kernel.org/stable/c/6bfc5377a210dbda2a237f16d94d1bd4f1335026, https://git.kernel.org/stable/c/7403f4118ab94be837ab9d770507537a8057bc63	O-LIN-LINU-020824/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about this is that TUR is not reading from the device. 2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808 ("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this first bounce buffer is allocated with GFP_ZERO. 3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we prepare as if the we had a DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtqueue_add_split() which uses DMA_FROM_DEVICE for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we first copy back the content of the second (that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce buffer, which contains all zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized,		

CVSS 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
			ain't all zeros and fails. One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all other participants are well behaved). Copying the content of the original buffer into the swiotlb buffer is the only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in doubt, but allow the driver to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance		

CVSS 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
			impact of the extra bounce. **CVE ID: CVE-2022-48853**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gianfar: ethtool: Fix refcount leak in gfar_get_ts_info The of_find_compatible_node() function returns a node pointer with refcount incremented, We should use of_node_put() on it when done Add the missing of_node_put() to release the refcount. **CVE ID: CVE-2022-48856**	https://git.kernel.org/stable/c/0e1b9a2078e07fb1e6e91bf8badfd89ecab1e848, https://git.kernel.org/stable/c/21044e679ed535345042d2023f7df0ca8e897e2a, https://git.kernel.org/stable/c/2ac5b58e645c66932438bb021cb5b52097ce70b0	O-LIN-LINU-020824/393
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in port100_send_complete	https://git.kernel.org/stable/c/0e721b8f2ee5e11376dd55363f9ccb539d754b8a, https://git.kernel.org/stable/c/205c4ec78e71cbf561794e6043da80e7bae6790f,	O-LIN-LINU-020824/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Syzbot reported UAF in port100_send_complete(). The root case is in missing usb_kill_urb() calls on error handling path of ->probe function. port100_send_complete() accesses devm allocated memory which will be freed on probe failure. We should kill this urbs before returning an error from probe function to prevent reported use-after-free Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540 by task ksoftirqd/2/26 ...	https://git.kernel.org/stable/c/2b1c85f56512d49e43bc53741fce2f508cd90029	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ... Allocated by task 1255:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ___kasan_kmalloc mm/kasan/common.c:515 [inline] ___kasan_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524 alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320 drivers/nfc/port100.c:1502 Freed by task 1255:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370 ___kasan_slab_free mm/kasan/common.c:366 [inline] ___kasan_slab_free+0xff/0x140 mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501 devres_release_all+0x114/0x190 drivers/base/devres.c:530		

CVSS 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
			really_probe+0x626/0xcc0 drivers/base/dd.c:670 **CVE ID: CVE-2022-48857**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do. **CVE ID: CVE-2022-48860**	https://git.kernel.org/stable/c/1852854ee349881efb78ccdbbb237838975902e4, https://git.kernel.org/stable/c/5e7c402892e189a7bc152b125e72261154aa585d, https://git.kernel.org/stable/c/669172ce976608b25a2f76f3c65d47f042d125c9	O-LIN-LINU-020824/395
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mISDN: Fix memory leak in dsp_pipeline_build()	https://git.kernel.org/stable/c/640445d6fc059d4514ffea79eb4196299e0e2d0f, https://git.kernel.org/stable/c/7777b1f795af1bb43867375d8a776080111aae1b,	O-LIN-LINU-020824/396

CVSS 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
			dsp_pipeline_build() allocates dup pointer by kstrdup(cfg), but then it updates dup variable by strsep(&dup, "|"). As a result when it calls kfree(dup), the dup variable contains NULL. Found by Linux Driver Verification project (linuxtesting.org) with SVACE. **CVE ID: CVE-2022-48863**	https://git.kernel.org/stable/c/a3d5fcc6cf2ecbba5a269631092570aa285a24cb	
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tipc: fix kernel panic when enabling bearer When enabling a bearer on a node, a kernel panic is observed: [4.498085] RIP: 0010:tipc_mon_prep+0x4e/0x130 [tipc] ...	https://git.kernel.org/stable/c/2de76d37d4a6dca9b96ea51da24d4290e6cfa1a5, https://git.kernel.org/stable/c/be4977b847f5d5cedb64d50eaaf2218c3a55a3a3, https://git.kernel.org/stable/c/f4f59fdbc748805b08c13dae14c01f0518c77c94	O-LIN-LINU-020824/397

CVSS 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
			[4.520030] Call Trace: [4.520689] <IRQ> [4.521236] tipc_link_build_proto_msg+0x375/0x750 [tipc] [4.522654] tipc_link_build_state_msg+0x48/0xc0 [tipc] [4.524034] __tipc_node_link_up+0xd7/0x290 [tipc] [4.525292] tipc_rcv+0x5da/0x730 [tipc] [4.526346] ? __netif_receive_skb_core+0xb7/0xfc0 [4.527601] tipc_l2_rcv_msg+0x5e/0x90 [tipc] [4.528737] __netif_receive_skb_list_core+0x20b/0x260 [4.530068] netif_receive_skb_list_internal+0x1bf/0x2e0 [4.531450] ? dev_gro_receive+0x4c2/0x680 [4.532512] napi_complete_done+0x6f/0x180		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4.533570] virtnet_poll+0x29c /0x42e [virtio_net] ... The node in question is receiving activate messages in another thread after changing bearer status to allow message sending/ receiving in current thread: thread 1 | thread 2 -------- | -------- | tipc_enable_bearer () | test_and_set_bit_lock() | tipc_bearer_xmit_skb() | | tipc_l2_rcv_msg() | tipc_rcv() | __tipc_node_link_up()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			| tipc_link_build_state_msg() | tipc_link_build_proto_msg() | tipc_mon_prep() | { | ... | // null-pointer dereference | u16 gen = mon->dom_gen; | ... | } // Not being executed yet | tipc_mon_create() | { | ... | // allocate | mon = kzalloc(); | ... | } | Monitoring pointer in thread 2 is dereferenced		

CVSS 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
			before monitoring data is allocated in thread 1. This causes kernel panic. This commit fixes it by allocating the monitoring data before enabling the bearer to receive messages. **CVE ID: CVE-2022-48865**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.30					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vrr: Set VRR capable prop only if it is attached to connector VRR capable property is not attached by default to the connector It is attached only if VRR is supported. So if the driver tries to call drm core set prop function without it being attached that causes NULL dereference.	https://git.kernel.org/stable/c/0ba557d330946c23559aaea2d51ea649fdeca98a, https://git.kernel.org/stable/c/3534c5c005ef99a1804ed50b8a72cdae254cabb5, https://git.kernel.org/stable/c/62929726ef0ec72cbbe9440c5d125d4278b99894	O-LIN-LINU-020824/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48843		
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting the following: [0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi)) [0.048183] ------------[cut here]------------ [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm:	https://git.kernel.org/stable/c/32813321f18d5432cec1b1a6ecc964f9ea26d565, https://git.kernel.org/stable/c/56eaacb8137ba2071ce48d4e3d91979270e139a7, https://git.kernel.org/stable/c/7315f8538db009605ffba00370678142ef00ac98	O-LIN-LINU-020824/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			swapper/1 Not tainted 5.17.0-rc3+ #35 b7b319f24073fd9a3c2aa7ad15fb7993eec0b26f [0.048247] Stack : 817f0000 00000004 327804c8 810eb050 00000000 00000004 00000000 c314fdd1 [0.048278] 830cbd64 819c0000 81800000 817f0000 83070bf4 00000001 830cbd08 00000000 [0.048307] 00000000 00000000 815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.048361] 817f0000 818a3c00 817f0000 00000004 00000000 00000000 4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/0x140 [0.048424] [<8131c2a0>] dump_stack_lvl+0x60/0x80 [0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>] warn_slowpath_fmt+0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_starting+0x198/0x240 [0.048483] [<810c6514>] sched_cpu_starting+0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callback_range+0x78/0x140		

CVSS 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
			[0.048510] [<8108d914>] notify_cpu_starting +0x94/0x140 [0.048523] [<8106593c>] start_secondary+0xbc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done. ...for each but CPU 0/boot. Basic debug printks right before the mentioned line say: [0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_starting() calculates core-scheduling parameters only		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			once per CPU start, and it's crucial to have all the parameters filled in at that moment (at least it uses cpu_smt_mask() which in fact is `&cpu_sibling_map[cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing the actual map calculation, was being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			callbacks in Linux 4.14 (see [0] for the reference). Neither me nor my brief tests couldn't find any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now yield exactly what I expected from them: [0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.org/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef **CVE ID: CVE-2022-48845**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.31					
N/A	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: usbtmc: Fix bug in pipe	https://git.kernel.org/stable/c/10a805334a11acd547602d6c4cf540a0f6ab5c6e, https://git.kernel.org/stable/c/	O-LIN-LINU-020824/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			direction for control transfers The syzbot fuzzer reported a minor bug in the usbtmc driver: usb 5-1: BOGUS control dir, pipe 80001e80 doesn't match bRequestType 0 WARNING: CPU: 0 PID: 3813 at drivers/usb/core/urb.c:412 usb_submit_urb+0x13a5/0x1970 drivers/usb/core/urb.c:410 Modules linked in: CPU: 0 PID: 3813 Comm: syz-executor122 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #0 ... Call Trace: <TASK> usb_start_wait_urb+0x113/0x530 drivers/usb/core/message.c:58 usb_internal_contr	5f6a2d63c68c12cf61259df7c3527a0e05dce952, https://git.kernel.org/stable/c/700a0715854c1e79a73341724ce4f5bb01abc016	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ol_msg drivers/usb/core/message.c:102 [inline] usb_control_msg+0x2a5/0x4b0 drivers/usb/core/message.c:153 usbtmc_ioctl_request drivers/usb/class/usbtmc.c:1947 [inline] The problem is that usbtmc_ioctl_request() uses usb_rcvctrlpipe() for all of its transfers, whether they are in or out. It's easy to fix. **CVE ID: CVE-2022-48834**		
Release of Invalid Pointer or Reference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Page fault in reply q processing A page fault was encountered in mpt3sas on a LUN reset error path:	https://git.kernel.org/stable/c/0cd2dd4bcf4abc812148c4943f966a3c8dccb00f, https://git.kernel.org/stable/c/3916e33b917581e2b2086e856c291cb86ea98a05, https://git.kernel.org/stable/c/69ad4ef868c1fc	O-LIN-LINU-020824/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[145.763216] mpt3sas_cm1: Task abort tm failed: handle(0x0002),timeout(30) tr_method(0x0) smid(3) msix_index(0) [145.778932] scsi 1:0:0:0: task abort: FAILED scmd(0x0000000024ba29a2) [145.817307] scsi 1:0:0:0: attempting device reset! scmd(0x0000000024ba29a2) [145.827253] scsi 1:0:0:0: [sg1] tag#2 CDB: Receive Diagnostic 1c 01 01 ff fc 00 [145.837617] scsi target1:0:0: handle(0x0002), sas_address(0x500605b0000272b9), phy(0) [145.848598] scsi target1:0:0: enclosure logical id(0x500605b0000272b8), slot(0) [149.858378] mpt3sas_cm1: Poll ReplyDescriptor queues for completion of smid(0),	7609daa235dfa46d28ba7a3ba3	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			task_type(0x05), handle(0x0002) [149.875202] BUG: unable to handle page fault for address: 00000007fffc445d [149.885617] #PF: supervisor read access in kernel mode [149.894346] #PF: error_code(0x0000) - not-present page [149.903123] PGD 0 P4D 0 [149.909387] Oops: 0000 [#1] PREEMPT SMP NOPTI [149.917417] CPU: 24 PID: 3512 Comm: scsi_eh_1 Kdump: loaded Tainted: G S O 5.10.89-altav-1 #1 [149.934327] Hardware name: DDN 200NVX2 /200NVX2-MB , BIOS ATHG2.2.02.01 09/10/2021 [149.951871] RIP: 0010:_base_process_reply_queue+0x4b/0x900 [mpt3sas] [149.961889] Code: 0f 84 22 02 00 00 8d 48 01 49 89 fd 48 8d 57 38 f0		

CVSS 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
			0f b1 4f 38 0f 85 d8 01 00 00 49 8b 45 10 45 31 e4 41 8b 55 0c 48 8d 1c d0 <0f> b6 03 83 e0 0f 3c 0f 0f 85 a2 00 00 00 e9 e6 01 00 00 0f b7 ee [149.991952] RSP: 0018:ffffc9000f1ebcb8 EFLAGS: 00010246 [150.000937] RAX: 0000000000000055 RBX: 00000007fffc445d RCX: 000000002548f071 [150.011841] RDX: 00000000ffff8881 RSI: 0000000000000001 RDI: ffff888125ed50d8 [150.022670] RBP: 0000000000000000 R08: 0000000000000000 R09: c0000000ffff7fff [150.033445] R10: ffffc9000f1ebb68 R11: ffffc9000f1ebb60 R12: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[150.044204] R13: ffff888125ed50d8 R14: 0000000000000080 R15: 34cdc00034cdea80 [150.054963] FS: 0000000000000000(0000) GS:ffff88dfaf200000(0000) knlGS:0000000000000000 [150.066715] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [150.076078] CR2: 00000007fffc445d CR3: 000000012448a006 CR4: 0000000000770ee0 [150.086887] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [150.097670] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[150.108323] PKRU: 55555554 [150.114690] Call Trace: [150.120497] ? printk+0x48/0x4a [150.127049] mpt3sas_scsih_issue_tm.cold.114+0x2e/0x2b3 [mpt3sas] [150.136453] mpt3sas_scsih_issue_locked_tm+0x86/0xb0 [mpt3sas] [150.145759] scsih_dev_reset+0xea/0x300 [mpt3sas] [150.153891] scsi_eh_ready_devs+0x541/0x9e0 [scsi_mod] [150.162206] ? __scsi_host_match+0x20/0x20 [scsi_mod] [150.170406] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.178925] ? blk_mq_tagset_busy_iter+0x45/0x60 [150.186638] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.195087] scsi_error_handler		

CVSS 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
			+0x3a5/0x4a0 [scsi_mod] [150.203206] ? __schedule+0x1e9/ 0x610 [150.209783] ? scsi_eh_get_sense+ 0x210/0x210 [scsi_mod] [150.217924] kthread+0x12e/0x 150 [150.224041] ? kthread_worker_fn +0x130/0x130 [150.231206] ret_from_fork+0x1f /0x30 This is caused by mpt3sas_base_sync _reply_irqs() using an invalid reply_q pointer outside of the list_for_each_entry( ) loop. At the end of the full list traversal the pointer is invalid. Move the _base_process_repl y_queue() call inside of the loop. **CVE ID: CVE-2022-48835**		
N/A	16-Jul-2024	5.5	In the Linux kernel, the following	https://git.kern el.org/stable/c/ 35069e654bcab	O-LIN-LINU-020824/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb() which is caused by wrong endpoint type. There was a check for the number of endpoints, but not for the type of endpoint. Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints Fail log: usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0	567ff8b9f0e68e1caf82c15dcd7, https://git.kernel.org/stable/c/5600f6986628dde888173409058847 4f54a540a8, https://git.kernel.org/stable/c/57277a8b5d881e02051ba9d7f6cb3f915c229821	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/usb/core/urb.c:502 Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ... Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320 drivers/input/input.c:629 kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593 **CVE ID: CVE-2022-48836**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/00bdd9bf1ac6d	O-LIN-LINU-020824/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug: BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-syzkaller-00229-g4f12b742eb2b #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline]	401ad926d3d8df41b9f1399f646, https://git.kernel.org/stable/c/16b1941eac2bd499f065a6739a40ce0011a3d740, https://git.kernel.org/stable/c/2015c23610cd0efadaeca4d3a8d1dae9a45aa35a	

CVSS 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
			dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 dev_uevent+0x712/0x780 drivers/base/core.c:2320 uevent_show+0x1b8/0x380 drivers/base/core.c:2391 dev_attr_show+0x4b/0x90 drivers/base/core.c:2094 Although the bug manifested in the driver core, the real cause was a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			race with the gadget core. dev_uevent() does:
			
			if (dev->driver)
			
			add_uevent_var(env, "DRIVER=%s", dev->driver->name);
			
			and between the test and the dereference of dev->driver, the gadget
			core sets dev->driver to NULL.
			
			The race wouldn't occur if the gadget core registered its devices on
			a real bus, using the standard synchronization techniques of the
			driver core. However, it's not necessary to make such a large change
			in order to fix this bug; all we need to do is make sure that
			udc->dev.driver is always NULL.
			
			In fact, there is no reason for udc-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>dev.driver ever to be set to anything, let alone to the value it currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC. This patch simply removes the statements in the gadget core that touch udc->dev.driver. **CVE ID: CVE-2022-48838**		
Out-of-bounds Read	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg() syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations,	https://git.kernel.org/stable/c/268dcf1f7b3193bc446ec3d14e08a240e9561e4d, https://git.kernel.org/stable/c/70b7b3c055fd4a464da8da55ff4c1f84269f9b02, https://git.kernel.org/stable/c/a055f5f2841f7522b44a2b1eccb1951b4b03d51a	O-LIN-LINU-020824/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tpacket_rcv() is queueing skbs with garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tainted 5.17.0-rc7-syzkaller-02396-g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+0x13d/0x180 mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline] packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ___sys_recvmsg+0x2c4/0x600 net/socket.c:2632 __sys_recvmsg+0x127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704		

CVSS 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
			do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 000000002000050		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ___sys_recvmsg+0x0/0x600 include/linux/uio.h:246 this frame has 1 object: [32, 160) 'addr'		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 >ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ========== **CVE ID: CVE-2022-48839**		
Affected Version(s): From (including) 5.13 Up to (excluding) 5.15.29					
Out-of-bounds Read	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/3ffbe85cda7f523dad896bae08cecd8db8b555ab,	O-LIN-LINU-020824/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HID: hid-thrustmaster: fix OOB read in thrustmaster_interrupts Syzbot reported an slab-out-of-bounds Read in thrustmaster_probe() bug. The root case is in missing validation check of actual number of endpoints. Code should not blindly access usb_host_interface::endpoint array, since it may contain less endpoints than code expects. Fix it by adding missing validaion check and print an error if number of endpoints do not match expected number **CVE ID: CVE-2022-48866**	https://git.kernel.org/stable/c/56185434e1e50acecee56d8f5850135009b87947, https://git.kernel.org/stable/c/fc3ef2e3297b3c0e2006b5d7b3d6696 5e3392036	
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/4b1743bc715a3691a63ac21b34	O-LIN-LINU-020824/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vdpa: fix use-after-free on vp_vdpa_remove When vp_vdpa driver is unbind, vp_vdpa is freed in vdpa_unregister_device and then vp_vdpa->mdev.pci_dev is dereferenced in vp_modern_remove, triggering use-after-free. Call Trace of unbinding driver free vp_vdpa : do_syscall_64 vfs_write kernfs_fop_write_iter device_release_driver_internal pci_device_remove vp_vdpa_remove vdpa_unregister_device kobject_release	9079b07bf1b19e, https://git.kernel.org/stable/c/dc54ba9932aeaaa1a21fe214af1f446593a78274, https://git.kernel.org/stable/c/eb057b44dbe35ae14527830236a92f51de8f9184	

CVSS 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
			device_release kfree Call Trace of dereference vp_vdpa->mdev.pci_dev: vp_modern_remove pci_release_selected_regions pci_release_region pci_resource_len pci_resource_end (dev)->resource[(bar)].end **CVE ID: CVE-2022-48861**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.29					
Use of Uninitialized Resource	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vdpa/mlx5: add validation for VIRTIO_NET_CTRL_MQ_VQ_PAIRS_SET command When control vq receives a VIRTIO_NET_CTRL	https://git.kernel.org/stable/c/9f6effca75626c7a7c7620dabcb1a254ca530230, https://git.kernel.org/stable/c/e7e118416465f2ba8b55007e5b789823e101421e, https://git.kernel.org/stable/c/ed0f849fc3a63e	O-LIN-LINU-020824/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_MQ_VQ_PAIRS_SET command request from the driver, presently there is no validation against the number of queue pairs to configure, or even if multiqueue had been negotiated or not is unverified. This may lead to kernel panic due to uninitialized resource for the queues were there any bogus request sent down by untrusted driver. Tie up the loose ends there. **CVE ID: CVE-2022-48864**	d2ddf5e72cdb1de3bdbbb0f8eb	
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.31					
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: release rq qos structures for queue without disk blkcg_init_queue() may add rq qos structures to	https://git.kernel.org/stable/c/60c2c8e2ef3a3ec79de8cbc80a06ca0c21df8c29, https://git.kernel.org/stable/c/d4ad8736ac982111bb0be8306bf19c8207f6600e, https://git.kernel.org/stable/c/daaca3522a8e6	O-LIN-LINU-020824/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request queue, previously blk_cleanup_queue () calls rq_qos_exit() to release them, but commit 8e141f9eb803 ("block: drain file system I/O on del_gendisk") moves rq_qos_exit() into del_gendisk(), so memory leak is caused because queues may not have disk, such as un-present scsi luns, nvme admin queue, ... Fixes the issue by adding rq_qos_exit() to blk_cleanup_queue () back. BTW, v5.18 won't need this patch any more since we move blkcg_init_queue()/ blkcg_exit_queue() into disk allocation/release handler, and patches have been in for-5.18/block.	7c46e39ef09c1d542e866f85f3b	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48846		
Affected Version(s): From (including) 5.15.24 Up to (excluding) 5.15.31					
Integer Overflow or Wraparound	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: prevent integer overflow in rndis_set_response() If "BufOffset" is very large the "BufOffset + 8" operation can have an integer overflow. **CVE ID: CVE-2022-48837**	https://git.kernel.org/stable/c/138d4f739b35dfb40438a0d5d7054965763bfbe7, https://git.kernel.org/stable/c/21829376268397f9fd2c35cfa9135937b6aa3a1e, https://git.kernel.org/stable/c/28bc0267399f42f987916a7174e2e32f0833cc65	O-LIN-LINU-020824/409
Affected Version(s): From (including) 5.15.27 Up to (excluding) 5.15.31					
Loop with Unreachable Exit Condition ('Infinite Loop')	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iavf: Fix hang during reboot/shutdown Recent commit 974578017fc1 ("iavf: Add waiting so the port is initialized in remove") adds a	https://git.kernel.org/stable/c/4477b9a4193b35eb3a8afd2adf2d42add2f88d57, https://git.kernel.org/stable/c/80974bb730270199c6fcb189af04d5945b87e813, https://git.kernel.org/stable/c/b04683ff8f0823b869c219c78ba	O-LIN-LINU-020824/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wait-loop at the beginning of iavf_remove() to ensure that port initialization is finished prior unregistering net device. This causes a regression in reboot/shutdown scenario because in this case callback iavf_shutdown() is called and this callback detaches the device, makes it down if it is running and sets its state to __IAVF_REMOVE. Later shutdown callback of associated PF driver (e.g. ice_shutdown) is called. That callback calls among other things sriov_disable() that calls indirectly iavf_remove() (see stack trace below). As the adapter state is already __IAVF_REMOVE then the mentioned loop is end-less and shutdown process hangs.	0d974bddea0b5	

CVSS 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 patch fixes this by checking adapter's state at the beginning of iavf_remove() and skips the rest of the function if the adapter is already in remove state (shutdown is in progress). Reproducer: 1. Create VF on PF driven by ice or i40e driver 2. Ensure that the VF is bound to iavf driver 3. Reboot [52625.981294] sysrq: SysRq : Show Blocked State [52625.988377] task:reboot state:D stack: 0 pid:17359 ppid: 1 f2 [52625.996732] Call Trace: [52625.999187] __schedule+0x2d1/0x830 [52626.007400] schedule+0x35/0xa0		

CVSS 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
			[52626.010545] schedule_hrtimeout_range_clock+0x83/0x100 [52626.020046] usleep_range+0x5b/0x80 [52626.023540] iavf_remove+0x63/0x5b0 [iavf] [52626.027645] pci_device_remove+0x3b/0xc0 [52626.031572] device_release_driver_internal+0x103/0x1f0 [52626.036805] pci_stop_bus_device+0x72/0xa0 [52626.040904] pci_stop_and_remove_bus_device+0xe/0x20 [52626.045870] pci_iov_remove_virtfn+0xba/0x120 [52626.050232] sriov_disable+0x2f/0xe0 [52626.053813] ice_free_vfs+0x7c/0x340 [ice] [52626.057946] ice_remove+0x220/0x240 [ice] [52626.061967] ice_shutdown+0x16/0x50 [ice]		

CVSS 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
			[52626.065987] pci_device_shutdown+0x34/0x60 [52626.070086] device_shutdown+0x165/0x1c5 [52626.074011] kernel_restart+0xe/0x30 [52626.077593] __do_sys_reboot+0x1d2/0x210 [52626.093815] do_syscall_64+0x5b/0x1a0 [52626.097483] entry_SYSCALL_64_after_hwframe+0x65/0xca **CVE ID: CVE-2022-48840**		
Affected Version(s): From (including) 5.16 Up to (excluding) 5.16.15					
Out-of-bounds Write	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: watch_queue: Fix filter limit check In watch_queue_set_filter(), there are a couple of places where we check that the filter type value does not exceed what the type_filter bitmap	https://git.kernel.org/stable/c/1b09f28f70a5046acd64138075ae3f095238b045, https://git.kernel.org/stable/c/648895da69ced90ca770fd941c3d9479a9d72c16, https://git.kernel.org/stable/c/b36588ebbcef74583824c08352e75838d6fb4ff2	O-LIN-LINU-020824/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			can hold. One place calculates the number of bits by:
			
			if (tf[i].type >= sizeof(wfilter->type_filter) * 8)
			
			which is fine, but the second does:
			
			if (tf[i].type >= sizeof(wfilter->type_filter) * BITS_PER_LONG)
			
			which is not. This can lead to a couple of out-of-bounds writes due to
			a too-large type:
			
			(1) __set_bit() on wfilter->type_filter
			(2) Writing more elements in wfilter->filters[] than we allocated.
			
			Fix this by just using the proper WATCH_TYPE__NR instead, which is the
			number of types we actually know about.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The bug may cause an oops looking something like: BUG: KASAN: slab-out-of-bounds in watch_queue_set_filter+0x659/0x740 Write of size 4 at addr ffff88800d2c66bc by task watch_queue_oob/611 ... Call Trace: <TASK> dump_stack_lvl+0x45/0x59 print_address_description.constprop.0+0x1f/0x150 ... kasan_report.cold+0x7f/0x11b ... watch_queue_set_filter+0x659/0x740 ... __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry_SYSCALL_64_after_hwframe+0x44/0xae Allocated by task 611: kasan_save_stack+0x1e/0x40 __kasan_kmalloc+0x81/0xa0 watch_queue_set_filter+0x23a/0x740 __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae The buggy address belongs to the object at ffff88800d2c66a0 which belongs to the cache kmalloc-32 of size 32 The buggy address is located 28 bytes inside of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			32-byte region [ffff88800d2c66a0, ffff88800d2c66c0) **CVE ID: CVE-2022-48847**		
N/A	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tracing/osnoise: Do not unregister events twice Nicolas reported that using: # trace-cmd record -e all -M 10 -p osnoise --poll Resulted in the following kernel warning: ------------[cut here]------------ WARNING: CPU: 0 PID: 1217 at kernel/tracepoint.c:404 tracepoint_probe_unregister+0x280/0x370 [...] CPU: 0 PID: 1217 Comm: trace-cmd Not tainted 5.17.0-rc6-next-	https://git.kernel.org/stable/c/4e10787d18379d9b296290c2288097feddef16d4, https://git.kernel.org/stable/c/f0cfe17bcc1dd2f0872966b554a148e888833ee9	O-LIN-LINU-020824/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20220307-nico+ #19 RIP: 0010:tracepoint_probe_unregister+0x280/0x370 [...] CR2: 00007ff919b29497 CR3: 0000000109da4005 CR4: 0000000000170ef0 Call Trace: <TASK> osnoise_workload_stop+0x36/0x90 tracing_set_tracer+0x108/0x260 tracing_set_trace_write+0x94/0xd0 ? __check_object_size.part.0+0x10a/0x150 ? selinux_file_permission+0x104/0x150 vfs_write+0xb5/0x290 ksys_write+0x5f/0xe0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0x3b/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7ff919a18127 [...] ---[end trace 0000000000000000]--- The warning complains about an attempt to unregister an unregistered tracepoint. This happens on trace-cmd because it first stops tracing, and then switches the tracer to nop. Which is equivalent to: # cd /sys/kernel/tracing/ # echo osnoise > current_tracer # echo 0 > tracing_on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			# echo nop > current_tracer The osnoise tracer stops the workload when no trace instance is actually collecting data. This can be caused both by disabling tracing or disabling the tracer itself. To avoid unregistering events twice, use the existing trace_osnoise_callback_enabled variable to check if the events (and the workload) are actually active before trying to deactivate them. **CVE ID: CVE-2022-48848**		
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: staging: gdm724x: fix use after free in gdm_lte_rx()	https://git.kernel.org/stable/c/1fb9dd3787495b4deb0efe66c58306b65691a48f, https://git.kernel.org/stable/c/403e3afe241b62401de1f8629c9c6b9b3d69dbf	O-LIN-LINU-020824/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len. **CVE ID: CVE-2022-48851**	f, https://git.kernel.org/stable/c/48ecdf3e29a6e514e8196691589c7dfc6c4ac169	
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: arc_emac: Fix use after free in arc_mdio_probe() If bus->state is equal to MDIOBUS_ALLOCATED, mdiobus_free(bus) will free the "bus". But bus->name is still used in the next line, which will lead to a use after free. We can fix it by putting the name in a local variable and make the bus->name point to the rodata section "name",then use the name in the error message without referring	https://git.kernel.org/stable/c/84c831803785c2c3bec5c28c0e8a0b72f6b41d4d, https://git.kernel.org/stable/c/bc0e610a6eb0d46e4123fafdbe5e6141d9fff3be	O-LIN-LINU-020824/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to bus to avoid the uaf. **CVE ID: CVE-2022-48854**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: sctp: fix kernel-infoleak for SCTP sockets syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill() calls inet_diag_msg_common_fill() Make sure to clear idiag_timer/idiag_retrans/idiag_expires and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1]	https://git.kernel.org/stable/c/1502f15b9f29c41883a6139f2923523873282a83, https://git.kernel.org/stable/c/2d8fa3fdf4542a2174a72d92018f488d65d848c5, https://git.kernel.org/stable/c/3fc0fd724d199e061432b66a8d85b7d48fe485f7	O-LIN-LINU-020824/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline] copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h:162 [inline] simple_copy_to_iter+0xf3/0x140 net/core/datagram.c:519 __skb_datagram_iter+0x2d5/0x11b0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/core/datagram.c:425 skb_copy_datagram_iter+0xdc/0x270 net/core/datagram.c:533 skb_copy_datagram_msg include/linux/skbuff.h:3696 [inline] netlink_recvmsg+0x669/0x1c80 net/netlink/af_netlink.c:1977 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x795/0xa10 net/socket.c:2097 __do_sys_recvfrom net/socket.c:2115 [inline] __se_sys_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom+0x19d/0x210 net/socket.c:2111		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_post_alloc_hook mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline] __kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline] __alloc_skb+0x545/0xf90 net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline] inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341 sock_diag_rcv_msg+0x24a/0x620 netlink_rcv_skb+0x40c/0x7e0 net/netlink/af_netlink.c:2494 sock_diag_rcv+0x63/0x80 net/core/sock_diag.c:277 netlink_unicast_kernel net/netlink/af_netlink.c:1317 [inline] netlink_unicast+0x1093/0x1360 net/netlink/af_netlink.c:1343		

CVSS 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
			netlink_sendmsg+0x14d9/0x1720 net/netlink/af_netlink.c:1919 sock_sendmsg_nosec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline] sock_write_iter+0x594/0x690 net/socket.c:1061 do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851 vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00 fs/read_write.c:967 __do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120		

CVSS 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
			fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000 Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not tainted 5.17.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 **CVE ID: CVE-2022-48855**		

CVSS 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
Out-of-bounds Read	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: HID: hid-thrustmaster: fix OOB read in thrustmaster_interrupts Syzbot reported an slab-out-of-bounds Read in thrustmaster_probe() bug. The root case is in missing validation check of actual number of endpoints. Code should not blindly access usb_host_interface::endpoint array, since it may contain less endpoints than code expects. Fix it by adding missing validaion check and print an error if number of endpoints do not match expected number	https://git.kernel.org/stable/c/3ffbe85cda7f523dad896bae08cecd8db8b555ab, https://git.kernel.org/stable/c/56185434e1e50acecee56d8f5850135009b87947, https://git.kernel.org/stable/c/fc3ef2e3297b3c0e2006b5d7b3d66965e3392036	O-LIN-LINU-020824/416

CVSS 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-2022-48866		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Jul-2024	7	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix a race on command flush flow Fix a refcount use after free warning due to a race on command entry. Such race occurs when one of the commands releases its last refcount and frees its index and entry while another process running command flush flow takes refcount to this command entry. The process which handles commands flush may see this command as needed to be flushed if the other process released its refcount but didn't release the index yet. Fix it by adding the needed spin lock.	https://git.kernel.org/stable/c/0401bfb27a91d7bdd74b1635c1aae57cbb128da6, https://git.kernel.org/stable/c/063bd355595428750803d8736a9bb7c8db67d42d, https://git.kernel.org/stable/c/1a4017926eeea56c7540cc41b42106746ee8a0ee	O-LIN-LINU-020824/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It fixes the following warning trace: refcount_t: addition on 0; use-after-free. WARNING: CPU: 11 PID: 540311 at lib/refcount.c:25 refcount_warn_saturate+0x80/0xe0 ... RIP: 0010:refcount_warn_saturate+0x80/0xe0 ... Call Trace: <TASK> mlx5_cmd_trigger_completions+0x293/0x340 [mlx5_core] mlx5_cmd_flush+0x3a/0xf0 [mlx5_core] enter_error_state+0x44/0x80 [mlx5_core] mlx5_fw_fatal_reporter_err_work+0x37/0xe0 [mlx5_core] process_one_work+0x1be/0x390		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			worker_thread+0x4d/0x3d0 ? rescuer_thread+0x350/0x350 kthread+0x141/0x160 ? set_kthread_struct+0x40/0x40 ret_from_fork+0x1f/0x30 </TASK> **CVE ID: CVE-2022-48858**		
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: bypass tiling flag check in virtual display case (v2) vkms leverages common amdgpu framebuffer creation, and also as it does not support FB modifier, there is no need to check tiling flags when initing	https://git.kernel.org/stable/c/cb29021be49858059138f75d6311a7c35a9379b2, https://git.kernel.org/stable/c/e2b993302f40c4eb714ecf896dd9e1c5be7d4cd7, https://git.kernel.org/stable/c/fcd1d79aa943fff4fbaa0cce1d576995a7960699	O-LIN-LINU-020824/418

CVSS 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
			framebuffer when virtual display is enabled. This can fix below calltrace: amdgpu 0000:00:08.0: GFX9+ requires FB check based on format modifier WARNING: CPU: 0 PID: 1023 at drivers/gpu/drm/amd/amdgpu/amdgpu_display.c:1150 amdgpu_display_framebuffer_init+0x8e7/0xb40 [amdgpu] v2: check adev->enable_virtual_display instead as vkms can be enabled in bare metal as well. **CVE ID: CVE-2022-48849**		
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show	https://git.kernel.org/stable/c/081369ad088a76429984483b8a5f7e967a125aad, https://git.kernel.org/stable/c/3a79f380b3e10edf6caa9aac901	O-LIN-LINU-020824/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When bringing down the netdevice or system shutdown, a panic can be triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0: Shutdown was called ... [757.937260] BUG: unable to handle kernel NULL pointer dereference at (null) [758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100	63a5d7a282204, https://git.kernel.org/stable/c/4224cfd7fb6523f7a9d1c8bb91bb5df1e38eb624	

CVSS 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 COMMAND: "amsd" ... #9 [ffff89240e1a38b0] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX: 0000000000001000 RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090 RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0		

CVSS 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: ffff89243d874090 R14: ffff89243d874080 R15: 0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core] #12 [ffff89240e1a3ab8] mlx5_cmd_exec at ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08] mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8] dev_attr_show at ffffffff8f0b70e3 #20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18] kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff		

CVSS 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
			#25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f #26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START|__LINK_STATE_NOCARRIER) To prevent this scenario, we also make sure that the netdevice is present. **CVE ID: CVE-2022-48850**		
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE The problem I'm addressing was discovered by the LTP test covering	https://git.kernel.org/stable/c/270475d6d2410ec66e971bf181afe1958dad565e, https://git.kernel.org/stable/c/6bfc5377a210dbda2a237f16d94d1bd4f1335026, https://git.kernel.org/stable/c/7403f4118ab94be837ab9d770	O-LIN-LINU-020824/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cve-2018-1000204. A short description of what happens follows: 1) The test case issues a command code 00 (TEST UNIT READY) via the SG_IO interface with: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_DEV and a corresponding dxferp. The peculiar thing about this is that TUR is not reading from the device. 2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808 ("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this	507537a8057bc63	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			first bounce buffer is allocated with GFP_ZERO. 3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we prepare as if the we had a DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function virtqueue_add_split() which uses DMA_FROM_DEVICE for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			first copy back the content of the second (that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce buffer, which contains all zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized, ain't all zeros and fails. One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all other participants are well behaved).		

CVSS 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
			Copying the content of the original buffer into the swiotlb buffer is the only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in doubt, but allow the driver to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance impact of the extra bounce. **CVE ID: CVE-2022-48853**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gianfar: ethtool: Fix refcount leak in gfar_get_ts_info The of_find_compatible_node() function returns a node pointer with	https://git.kernel.org/stable/c/0e1b9a2078e07fb1e6e91bf8badfd89ecab1e848, https://git.kernel.org/stable/c/21044e679ed535345042d2023f7df0ca8e897e2a, https://git.kernel.org/stable/c/2ac5b58e645c66932438bb021	O-LIN-LINU-020824/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refcount incremented, We should use of_node_put() on it when done Add the missing of_node_put() to release the refcount. **CVE ID: CVE-2022-48856**	cb5b52097ce70b0	
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in port100_send_complete Syzbot reported UAF in port100_send_complete(). The root case is in missing usb_kill_urb() calls on error handling path of ->probe function. port100_send_complete() accesses devm allocated memory which will be freed on probe failure. We should	https://git.kernel.org/stable/c/0e721b8f2ee5e11376dd55363f9ccb539d754b8a, https://git.kernel.org/stable/c/205c4ec78e71cbf561794e6043da80e7bae6790f, https://git.kernel.org/stable/c/2b1c85f56512d49e43bc53741fce2f508cd90029	O-LIN-LINU-020824/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kill this urbs before returning an error from probe function to prevent reported use-after-free Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540 by task ksoftirqd/2/26 ... Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ... Allocated by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ___kasan_kmalloc mm/kasan/common.c:515 [inline]		

CVSS 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_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524 alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320 drivers/nfc/port100.c:1502 Freed by task 1255: kasan_save_stack+0x1e/0x40 mm/kasan/common.c:38 kasan_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30		

CVSS 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
			mm/kasan/generic.c:370 ___kasan_slab_free mm/kasan/common.c:366 [inline] ___kasan_slab_free+0xff/0x140 mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501 devres_release_all+0x114/0x190 drivers/base/devres.c:530 really_probe+0x626/0xcc0 drivers/base/dd.c:670 **CVE ID: CVE-2022-48857**		
Missing Release of Memory after	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/4cc66bf17220ff9631f9fa99b02a872e0ad5a08b,	O-LIN-LINU-020824/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			net: marvell: prestera: Add missing of_node_put() in prestera_switch_set_base_mac_addr This node pointer is returned by of_find_compatible_node() with refcount incremented. Calling of_node_put() to aovid the refcount leak. **CVE ID: CVE-2022-48859**	https://git.kernel.org/stable/c/b7c2fd1d126329340639adfb8dd2938fe4b65df7, https://git.kernel.org/stable/c/c9ffa3e2bc451816ce0295e40063514fabf2bd36	
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do.	https://git.kernel.org/stable/c/1852854ee349881efb78ccdbbb237838975902e4, https://git.kernel.org/stable/c/5e7c402892e189a7bc152b125e72261154aa585d, https://git.kernel.org/stable/c/669172ce976608b25a2f76f3c65d47f042d125c9	O-LIN-LINU-020824/424

CVSS 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-2022-48860		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vdpa: fix use-after-free on vp_vdpa_remove When vp_vdpa driver is unbind, vp_vdpa is freed in vdpa_unregister_device and then vp_vdpa->mdev.pci_dev is dereferenced in vp_modern_remove, triggering use-after-free. Call Trace of unbinding driver free vp_vdpa : do_syscall_64 vfs_write kernfs_fop_write_iter device_release_driver_internal pci_device_remove vp_vdpa_remove	https://git.kernel.org/stable/c/4b1743bc715a3691a63ac21b349079b07bf1b19e, https://git.kernel.org/stable/c/dc54ba9932aeaaa1a21fe214af1f446593a78274, https://git.kernel.org/stable/c/eb057b44dbe35ae14527830236a92f51de8f9184	O-LIN-LINU-020824/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vdpa_unregister_device kobject_release device_release kfree Call Trace of dereference vp_vdpa->mdev.pci_dev: vp_modern_remove pci_release_selected_regions pci_release_region pci_resource_len pci_resource_end (dev)->resource[(bar)].end **CVE ID: CVE-2022-48861**		
Loop with Unreachable Exit Condition ('Infinite Loop')	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vhost: fix hung thread due to erroneous iotlb entries	https://git.kernel.org/stable/c/d9a747e6b6561280bf1791bb24c5e9e082193dad, https://git.kernel.org/stable/c/e2ae38cf3d91837a493cb2093c87700ff3cbe66	O-LIN-LINU-020824/426

CVSS 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 vhost_iotlb_add_range_ctx(), range size can overflow to 0 when start is 0 and last is ULONG_MAX. One instance where it can happen is when userspace sends an IOTLB message with iova=size=uaddr=0 (vhost_process_iotlb_msg). So, an entry with size = 0, start = 0, last = ULONG_MAX ends up in the iotlb. Next time a packet is sent, iotlb_access_ok() loops indefinitely due to that erroneous entry. Call Trace: <TASK> iotlb_access_ok+0x21b/0x3e0 drivers/vhost/vhost.c:1340 vq_meta_prefetch+0xbc/0x280 drivers/vhost/vhost.c:1366	7, https://git.kernel.org/stable/c/f8d88e86e90ea1002226d7ac2430152bfea003d1	

CVSS 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
			vhost_transport_do_send_pkt+0xe0/0xfd0 drivers/vhost/vsock.c:104 vhost_worker+0x23d/0x3d0 drivers/vhost/vhost.c:372 kthread+0x2e9/0x3a0 kernel/kthread.c:377 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 </TASK> Reported by syzbot at: https://syzkaller.appspot.com/bug?extid=0abd373e2e50d704db87 To fix this, do two things: 1. Return -EINVAL in vhost_chr_write_iter() when userspace asks to map a range with size 0.		

CVSS 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
			2. Fix vhost_iotlb_add_range_ctx() to handle the range [0, ULONG_MAX] by splitting it into two entries. **CVE ID: CVE-2022-48862**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mISDN: Fix memory leak in dsp_pipeline_build() dsp_pipeline_build() allocates dup pointer by kstrdup(cfg), but then it updates dup variable by strsep(&dup, "|"). As a result when it calls kfree(dup), the dup variable contains NULL. Found by Linux Driver Verification project (linuxtesting.org) with SVACE. **CVE ID: CVE-2022-48863**	https://git.kernel.org/stable/c/640445d6fc059d4514ffea79eb4196299e0e2d0f, https://git.kernel.org/stable/c/7777b1f795af1bb43867375d8a776080111aae1b, https://git.kernel.org/stable/c/a3d5fcc6cf2ecbba5a269631092570aa285a24cb	O-LIN-LINU-020824/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vdpa/mlx5: add validation for VIRTIO_NET_CTRL_MQ_VQ_PAIRS_SET command When control vq receives a VIRTIO_NET_CTRL_MQ_VQ_PAIRS_SET command request from the driver, presently there is no validation against the number of queue pairs to configure, or even if multiqueue had been negotiated or not is unverified. This may lead to kernel panic due to uninitialized resource for the queues were there any bogus request sent down by untrusted driver. Tie up the loose ends there. **CVE ID: CVE-2022-48864**	https://git.kernel.org/stable/c/9f6effca75626c7a7c7620dabcb1a254ca530230, https://git.kernel.org/stable/c/e7e118416465f2ba8b55007e5b789823e101421e, https://git.kernel.org/stable/c/ed0f849fc3a63ed2ddf5e72cdb1de3bdbbb0f8eb	O-LIN-LINU-020824/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: tipc: fix kernel panic when enabling bearer When enabling a bearer on a node, a kernel panic is observed: [4.498085] RIP: 0010:tipc_mon_prep+0x4e/0x130 [tipc] ... [4.520030] Call Trace: [4.520689] <IRQ> [4.521236] tipc_link_build_proto_msg+0x375/0x750 [tipc] [4.522654] tipc_link_build_state_msg+0x48/0xc0 [tipc] [4.524034] __tipc_node_link_up+0xd7/0x290 [tipc] [4.525292] tipc_rcv+0x5da/0x730 [tipc]	https://git.kernel.org/stable/c/2de76d37d4a6dca9b96ea51da24d4290e6cfa1a5, https://git.kernel.org/stable/c/be4977b847f5d5cedb64d50eaaf2218c3a55a3a3, https://git.kernel.org/stable/c/f4f59fdbc748805b08c13dae14c01f0518c77c94	O-LIN-LINU-020824/429

CVSS 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
			[4.526346] ? __netif_receive_skb _core+0xb7/0xfc0 [4.527601] tipc_l2_rcv_msg+0x 5e/0x90 [tipc] [4.528737] __netif_receive_skb _list_core+0x20b/0 x260 [4.530068] netif_receive_skb_li st_internal+0x1bf/ 0x2e0 [4.531450] ? dev_gro_receive+0 x4c2/0x680 [4.532512] napi_complete_don e+0x6f/0x180 [4.533570] virtnet_poll+0x29c /0x42e [virtio_net] ... The node in question is receiving activate messages in another thread after changing bearer status to allow message sending/ receiving in current thread: thread 1 | thread 2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			-------- | -------- | tipc_enable_bearer() | test_and_set_bit_lock() | tipc_bearer_xmit_skb() | tipc_l2_rcv_msg() | tipc_rcv() | __tipc_node_link_up() | tipc_link_build_state_msg() | tipc_link_build_proto_msg() | tipc_mon_prep() | { | ... | // null-pointer dereference | u16 gen = mon->dom_gen; | ...		

CVSS 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 being executed yet |
			tipc_mon_create() |
			{ |
			... |
			// allocate |
			mon = kzalloc(); |
			... |
			} |
			
			Monitoring pointer in thread 2 is dereferenced before monitoring data
			is allocated in thread 1. This causes kernel panic.
			
			This commit fixes it by allocating the monitoring data before enabling
			the bearer to receive messages.
			CVE ID: CVE-2022-48865		

N/A	16-Jul-2024	3.3	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1ed68d776246f167aee9cd79f63f089c40a5e2a3, https://git.kern	O-LIN-LINU-020824/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/vc4: hdmi: Unregister codec device on unbind On bind we will register the HDMI codec device but we don't unregister it on unbind, leading to a device leakage. Unregister our device at unbind. **CVE ID: CVE-2022-48852**	el.org/stable/c/e40945ab7c7f966d0c37b7bd7b0596497dfe228d, https://git.kernel.org/stable/c/ee22082c3e2f230028afa0e22aa8773b1de3c919	
Affected Version(s): From (including) 5.16 Up to (excluding) 5.16.16					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vrr: Set VRR capable prop only if it is attached to connector VRR capable property is not attached by default to the connector It is attached only if VRR is supported. So if the driver tries to call drm core set prop function without it being attached that causes NULL dereference.	https://git.kernel.org/stable/c/0ba557d330946c23559aaea2d51ea649fdeca98a, https://git.kernel.org/stable/c/3534c5c005ef99a1804ed50b8a72cdae254cabb5, https://git.kernel.org/stable/c/62929726ef0ec72cbbe9440c5d125d4278b99894	O-LIN-LINU-020824/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48843		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: Fix leaking sent_cmd skb sent_cmd memory is not freed before freeing hci_dev causing it to leak it contents. **CVE ID: CVE-2022-48844**	https://git.kernel.org/stable/c/3679ccc09d8806686d579095ed504e045af7f7d6, https://git.kernel.org/stable/c/9473d06bd1c8da49eafb685aa95a290290c672dd, https://git.kernel.org/stable/c/dd3b1dc3dd050f1f47cd13e30073285241427 0f8	O-LIN-LINU-020824/432
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting the following:	https://git.kernel.org/stable/c/32813321f18d5432cec1b1a6ecc964f9ea26d565, https://git.kernel.org/stable/c/56eaacb8137ba2071ce48d4e3d91979270e139a7, https://git.kernel.org/stable/c/7315f8538db009605ffba00370678142ef00ac98	O-LIN-LINU-020824/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi)) [0.048183] ----------[cut here]---------- [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc3+ #35 b7b319f24073fd9a3c2aa7ad15fb7993eec0b26f [0.048247] Stack : 817f0000 00000004 327804c8 810eb050 00000000 00000004 00000000 c314fdd1 [0.048278] 830cbd64 819c0000 81800000 817f0000 83070bf4 00000001		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			830cbd08 00000000 [0.048307] 00000000 00000000 815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34 [0.048361] 817f0000 818a3c00 817f0000 00000004 00000000 00000000 4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/0x140 [0.048424] [<8131c2a0>] dump_stack_lvl+0x60/0x80		

CVSS 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
			[0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>] warn_slowpath_fmt +0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_starting+0x198/0x240 [0.048483] [<810c6514>] sched_cpu_starting +0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callback_range+0x78/0x140 [0.048510] [<8108d914>] notify_cpu_starting +0x94/0x140 [0.048523] [<8106593c>] start_secondary+0xbc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done.		

CVSS 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
			...for each but CPU 0/boot. Basic debug printks right before the mentioned line say: [0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_starting() calculates core-scheduling parameters only once per CPU start, and it's crucial to have all the parameters filled in at that moment (at least it uses cpu_smt_mask() which in fact is `&cpu_sibling_map[cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing the actual map calculation, was		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP callbacks in Linux 4.14 (see [0] for the reference). Neither me nor my brief tests couldn't find any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now yield exactly what I expected from them:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.org/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef **CVE ID: CVE-2022-48845**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Jul-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: ice: Fix race condition during interface enslave Commit 5dbbbd01cbba83 ("ice: Avoid RTNL lock when re-creating auxiliary device") changes a process of re-creation of aux device so ice_plug_aux_dev() is called from ice_service_task() context. This unfortunately opens a race window that can result in dead-lock	https://git.kernel.org/stable/c/5cb1ebdbc4342b1c2ce89516e19808d64417bdbc, https://git.kernel.org/stable/c/a9bbacc53d1f5ed8febbfdf31401d20e005f49ef, https://git.kernel.org/stable/c/e1014fc5572375658fa421531cedb6e084f477dc	O-LIN-LINU-020824/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			when interface has left LAG and immediately enters LAG again.
			
			Reproducer:
			``
			#!/bin/sh
			
			ip link add lag0 type bond mode 1 miimon 100
			ip link set lag0
			
			for n in {1..10}; do
			echo Cycle: $n
			ip link set ens7f0 master lag0
			sleep 1
			ip link set ens7f0 nomaster
			done
			``
			
			This results in:
			[20976.208697] Workqueue: ice ice_service_task [ice]
			[20976.213422] Call Trace:
			[20976.215871] __schedule+0x2d1/0x830
			[20976.219364] schedule+0x35/0xa0		

CVSS 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
			[20976.222510] schedule_preempt_disabled+0xa/0x10 [20976.227043] __mutex_lock.isra.7+0x310/0x420 [20976.235071] enum_all_gids_of_dev_cb+0x1c/0x100 [ib_core] [20976.251215] ib_enum_roce_netdev+0xa4/0xe0 [ib_core] [20976.256192] ib_cache_setup_one+0x33/0xa0 [ib_core] [20976.261079] ib_register_device+0x40d/0x580 [ib_core] [20976.266139] irdma_ib_register_device+0x129/0x250 [irdma] [20976.281409] irdma_probe+0x2c1/0x360 [irdma] [20976.285691] auxiliary_bus_probe+0x45/0x70 [20976.289790] really_probe+0x1f2/0x480 [20976.298509] driver_probe_device+0x49/0xc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[20976.302609] bus_for_each_drv+0x79/0xc0 [20976.306448] __device_attach+0xdc/0x160 [20976.310286] bus_probe_device+0x9d/0xb0 [20976.314128] device_add+0x43c/0x890 [20976.321287] __auxiliary_device_add+0x43/0x60 [20976.325644] ice_plug_aux_dev+0xb2/0x100 [ice] [20976.330109] ice_service_task+0xd0c/0xed0 [ice] [20976.342591] process_one_work+0x1a7/0x360 [20976.350536] worker_thread+0x30/0x390 [20976.358128] kthread+0x10a/0x120 [20976.365547] ret_from_fork+0x1f/0x40 ... [20976.438030] task:ip state:D stack: 0 pid:213658 ppid:213627 flags:0x00004084		

CVSS 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
			[20976.446469] Call Trace: [20976.448921] __schedule+0x2d1/0x830 [20976.452414] schedule+0x35/0xa0 [20976.455559] schedule_preempt_disabled+0xa/0x10 [20976.460090] __mutex_lock.isra.7+0x310/0x420 [20976.464364] device_del+0x36/0x3c0 [20976.467772] ice_unplug_aux_dev+0x1a/0x40 [ice] [20976.472313] ice_lag_event_handler+0x2a2/0x520 [ice] [20976.477288] notifier_call_chain+0x47/0x70 [20976.481386] __netdev_upper_dev_link+0x18b/0x280 [20976.489845] bond_enslave+0xe05/0x1790 [bonding] [20976.494475] do_setlink+0x336/0xf50		

CVSS 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
			[20976.502517] __rtnl_newlink+0x529/0x8b0 [20976.543441] rtnl_newlink+0x43/0x60 [20976.546934] rtnetlink_rcv_msg+0x2b1/0x360 [20976.559238] netlink_rcv_skb+0x4c/0x120 [20976.563079] netlink_unicast+0x196/0x230 [20976.567005] netlink_sendmsg+0x204/0x3d0 [20976.570930] sock_sendmsg+0x4c/0x50 [20976.574423] ___sys_sendmsg+0x1eb/0x250 [20976.586807] ___sys_sendmsg+0x7c/0xc0 [20976.606353] __sys_sendmsg+0x57/0xa0 [20976.609930] do_syscall_64+0x5b/0x1a0 [20976.613598] entry_SYSCALL_64_after_hwframe+0x65/0xca 1. Command 'ip link ... set nomaster'		

CVSS 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
			causes that ice_plug_aux_dev() is called from ice_service_task() context, aux device is created and associated device->lock is taken. 2. Command 'ip link ... set master...' calls ice's notifier under RTNL lock and that notifier calls ice_unplug_aux_dev(). That function tries to take aux device->lock but this is already taken by ice_plug_aux_dev() in step 1 3. Later ice_plug_aux_dev() tries to take RTNL lock but this is already taken in step 2 4. Dead-lock The patch fixes this issue by following changes: - Bit ICE_FLAG_PLUG_AUX_DEV is kept to be set during ice_plug_aux_dev()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			call in ice_service_task() - The bit is checked in ice_clear_rdma_cap() and only if it is not set then ice_unplug_aux_dev() is called. If it is set (in other words plugging of aux device was requested and ice_plug_aux_dev() is potentially running) then the function only clears the ---truncated--- **CVE ID: CVE-2022-48842**		
Affected Version(s): From (including) 5.16 Up to (excluding) 5.16.17					
Release of Invalid Pointer or Reference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Page fault in reply q processing A page fault was encountered in mpt3sas on a LUN reset error path:	https://git.kernel.org/stable/c/0cd2dd4bcf4abc812148c4943f966a3c8dccb00f, https://git.kernel.org/stable/c/3916e33b917581e2b2086e856c291cb86ea98a05, https://git.kernel.org/stable/c/69ad4ef868c1fc7609daa235dfa46d28ba7a3ba3	O-LIN-LINU-020824/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[145.763216] mpt3sas_cm1: Task abort tm failed: handle(0x0002),timeout(30) tr_method(0x0) smid(3) msix_index(0) [145.778932] scsi 1:0:0:0: task abort: FAILED scmd(0x0000000024ba29a2) [145.817307] scsi 1:0:0:0: attempting device reset! scmd(0x0000000024ba29a2) [145.827253] scsi 1:0:0:0: [sg1] tag#2 CDB: Receive Diagnostic 1c 01 01 ff fc 00 [145.837617] scsi target1:0:0: handle(0x0002), sas_address(0x500605b0000272b9), phy(0) [145.848598] scsi target1:0:0: enclosure logical id(0x500605b0000272b8), slot(0) [149.858378] mpt3sas_cm1: Poll ReplyDescriptor queues for completion of smid(0), task_type(0x05), handle(0x0002)		

CVSS 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
			[149.875202] BUG: unable to handle page fault for address: 00000007fffc445d [149.885617] #PF: supervisor read access in kernel mode [149.894346] #PF: error_code(0x0000) - not-present page [149.903123] PGD 0 P4D 0 [149.909387] Oops: 0000 [#1] PREEMPT SMP NOPTI [149.917417] CPU: 24 PID: 3512 Comm: scsi_eh_1 Kdump: loaded Tainted: G S O 5.10.89-altav-1 #1 [149.934327] Hardware name: DDN 200NVX2 /200NVX2-MB , BIOS ATHG2.2.02.01 09/10/2021 [149.951871] RIP: 0010:_base_process_reply_queue+0x4b/0x900 [mpt3sas] [149.961889] Code: 0f 84 22 02 00 00 8d 48 01 49 89 fd 48 8d 57 38 f0 0f b1 4f 38 0f 85 d8 01 00 00 49 8b 45		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10 45 31 e4 41 8b 55 0c 48 8d 1c d0 <0f> b6 03 83 e0 0f 3c 0f 0f 85 a2 00 00 00 e9 e6 01 00 00 0f b7 ee [149.991952] RSP: 0018:ffffc9000f1ebcb8 EFLAGS: 00010246 [150.000937] RAX: 0000000000000055 RBX: 00000007fffc445d RCX: 000000002548f071 [150.011841] RDX: 00000000ffff8881 RSI: 0000000000000001 RDI: ffff888125ed50d8 [150.022670] RBP: 0000000000000000 R08: 0000000000000000 R09: c0000000ffff7fff [150.033445] R10: ffffc9000f1ebb68 R11: ffffc9000f1ebb60 R12: 0000000000000000 [150.044204] R13: ffff888125ed50d8 R14:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000080 R15: 34cdc00034cdea80 [150.054963] FS: 0000000000000000(0000) GS:ffff88dfaf200000(0000) knlGS:0000000000000000 [150.066715] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [150.076078] CR2: 00000007fffc445d CR3: 000000012448a006 CR4: 0000000000770ee0 [150.086887] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [150.097670] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [150.108323] PKRU: 55555554		

CVSS 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
			[150.114690] Call Trace: [150.120497] ? printk+0x48/0x4a [150.127049] mpt3sas_scsih_issue_tm.cold.114+0x2e/0x2b3 [mpt3sas] [150.136453] mpt3sas_scsih_issue_locked_tm+0x86/0xb0 [mpt3sas] [150.145759] scsih_dev_reset+0xea/0x300 [mpt3sas] [150.153891] scsi_eh_ready_devs+0x541/0x9e0 [scsi_mod] [150.162206] ? __scsi_host_match+0x20/0x20 [scsi_mod] [150.170406] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.178925] ? blk_mq_tagset_busy_iter+0x45/0x60 [150.186638] ? scsi_try_target_reset+0x90/0x90 [scsi_mod] [150.195087] scsi_error_handler+0x3a5/0x4a0 [scsi_mod]		

CVSS 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
			[150.203206] ? __schedule+0x1e9/ 0x610 [150.209783] ? scsi_eh_get_sense+ 0x210/0x210 [scsi_mod] [150.217924] kthread+0x12e/0x 150 [150.224041] ? kthread_worker_fn +0x130/0x130 [150.231206] ret_from_fork+0x1f /0x30 This is caused by mpt3sas_base_sync _reply_irqs() using an invalid reply_q pointer outside of the list_for_each_entry( ) loop. At the end of the full list traversal the pointer is invalid. Move the _base_process_repl y_queue() call inside of the loop. **CVE ID: CVE-2022-48835**		
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 35069e654bcab 567ff8b9f0e68e 1caf82c15dcd7,	O-LIN-LINU-020824/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb() which is caused by wrong endpoint type. There was a check for the number of endpoints, but not for the type of endpoint. Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints Fail log: usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502	https://git.kernel.org/stable/c/5600f6986628dde888173409058847 4f54a540a8, https://git.kernel.org/stable/c/57277a8b5d881e02051ba9d7f6cb3f915c229821	

CVSS 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
			Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ... Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320 drivers/input/input.c:629 kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593 **CVE ID: CVE-2022-48836**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/00bdd9bf1ac6d401ad926d3d8df41b9f1399f64	O-LIN-LINU-020824/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug: BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-syzkaller-00229-g4f12b742eb2b #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134	6, https://git.kernel.org/stable/c/16b1941eac2bd499f065a6739a40ce0011a3d740, https://git.kernel.org/stable/c/2015c23610cd0efadaeca4d3a8d1dae9a45aa35a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 dev_uevent+0x712/0x780 drivers/base/core.c:2320 uevent_show+0x1b8/0x380 drivers/base/core.c:2391 dev_attr_show+0x4b/0x90 drivers/base/core.c:2094 Although the bug manifested in the driver core, the real cause was a race with the gadget core. dev_uevent() does:		

CVSS 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 (dev->driver)
			
			add_uevent_var(env, "DRIVER=%s", dev->driver->name);
			
			and between the test and the dereference of dev->driver, the gadget
			core sets dev->driver to NULL.
			
			The race wouldn't occur if the gadget core registered its devices on
			a real bus, using the standard synchronization techniques of the
			driver core. However, it's not necessary to make such a large change
			in order to fix this bug; all we need to do is make sure that
			udc->dev.driver is always NULL.
			
			In fact, there is no reason for udc->dev.driver ever to be set to
			anything, let alone to the value it		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC. This patch simply removes the statements in the gadget core that touch udc->dev.driver. **CVE ID: CVE-2022-48838**		
Out-of-bounds Read	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg() syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations, tpacket_rcv() is queueing skbs with	https://git.kernel.org/stable/c/268dcf1f7b3193bc446ec3d14e08a240e9561e4d, https://git.kernel.org/stable/c/70b7b3c055fd4a464da8da55ff4c1f84269f9b02, https://git.kernel.org/stable/c/a055f5f2841f7522b44a2b1eccb1951b4b03d51a	O-LIN-LINU-020824/438

CVSS 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
			garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not tainted 5.17.0-rc7-syzkaller-02396-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0x13d/0x180		

CVSS 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
			mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline] packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ___sys_recvmsg+0x2c4/0x600 net/socket.c:2632 __sys_recvmsg+0x127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704		

CVSS 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
			do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 000000002000050		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ___sys_recvmsg+0x0/0x600 include/linux/uio.h:246 this frame has 1 object: [32, 160) 'addr'		

CVSS 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
			Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 >ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ========== **CVE ID: CVE-2022-48839**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/60c2c8e2ef3a3ec79de8cbc80a06ca0c21df8c29, https://git.kernel.org/stable/c/d4ad8736ac982	O-LIN-LINU-020824/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			block: release rq qos structures for queue without disk blkcg_init_queue() may add rq qos structures to request queue, previously blk_cleanup_queue() calls rq_qos_exit() to release them, but commit 8e141f9eb803 ("block: drain file system I/O on del_gendisk") moves rq_qos_exit() into del_gendisk(), so memory leak is caused because queues may not have disk, such as un-present scsi luns, nvme admin queue, ... Fixes the issue by adding rq_qos_exit() to blk_cleanup_queue() back. BTW, v5.18 won't need this patch any more since we move	111bb0be8306bf19c8207f6600e, https://git.kernel.org/stable/c/daaca3522a8e67c46e39ef09c1d542e866f85f3b	

CVSS 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
			blkcg_init_queue()/ blkcg_exit_queue() into disk allocation/release handler, and patches have been in for-5.18/block. **CVE ID: CVE-2022-48846**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.97					
Unchecked Return Value	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into account with bpf_prog_lock_ro() set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error. **CVE ID: CVE-2024-42068**	https://git.kernel.org/stable/c/05412471beba313ecded95aa17b25fe84bb2551a, https://git.kernel.org/stable/c/7d2cc63eca0c993c99d18893214abf8f85d566d8, https://git.kernel.org/stable/c/a359696856ca9409fb97655c5a8ef0f549cb6e03	O-LIN-LINU-020824/440
Missing Release of Memory after Effective Lifetime	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE	https://git.kernel.org/stable/c/23752737c6a618e994f9a310ec2568881a6b49c4, https://git.kernel.org/stable/c/40188a25a984	O-LIN-LINU-020824/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers. **CVE ID: CVE-2024-42070**	7dbeb7ec67517174a835a677752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b5153848bfa1c2980f	
Use of Uninitialized Resource	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in	https://git.kernel.org/stable/c/4c5dc3927e17489c1cae6f48c0d5e4acb4cae01f, https://git.kernel.org/stable/c/5e4ed38eb17eaca42de57d500cc0f9668d2b6abf, https://git.kern	O-LIN-LINU-020824/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance	el.org/stable/c/a2a0ebff7fdeb2f66e29335adf64b9e457300dd4	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ___sys_recvmsg+0x18a/0x620 net/socket.c:2803 __sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50		

CVSS 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
			arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668		

CVSS 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
			alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ___sys_sendmsg+0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized		

CVSS 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
			Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 **CVE ID: CVE-2024-42076**		
N/A	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using	https://git.kernel.org/stable/c/320273b5649bbcee87f9e65343077189699d2a7a, https://git.kernel.org/stable/c/331d1079d58206ff7dc5518185f800b412f89bc6, https://git.kernel.org/stable/c/9ea2d1c6789722d58ec191f14f9a02518d55b6b4	O-LIN-LINU-020824/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in		

CVSS 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
			jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 filesystem. To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2] #4 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7		

CVSS 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
			#12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba **CVE ID: CVE-2024-42077**		
Out-of-bounds Write	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/782bdaf9d01658281bc813f3f873e6258aa1fd8d,	O-LIN-LINU-020824/444

CVSS 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
			RDMA/restrack: Fix potential invalid address access struct rdma_restrack_entry's kern_name was set to KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this rdma_restrack_entry, it would cause a invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one forgotten PD release in one of the ULPs. But it is not needed anymore, so delete them. **CVE ID: CVE-2024-42080**	https://git.kernel.org/stable/c/8656ef8a9288d6c932654f8d3856dc4ab1cfc6b5, https://git.kernel.org/stable/c/8ac281d42337f36cf7061cf1ea094181b84bc1a9	
Allocation of Resources Without Limits or Throttling	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1095b8efbb13a6a5fa583ed373ee1ccab29da2d0, https://git.kern	O-LIN-LINU-020824/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation.	el.org/stable/c/14e51ea78b4ccacb7acb1346b9241bb790a2054c, https://git.kernel.org/stable/c/1d3e3b3aa2cbe9bc7db9a7f8673a9fa6d2990d54	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thus, there is no sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_mod		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			el+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_live+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736		

CVSS 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
			do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Found by Linux Verification Center (linuxtesting.org) with syzkaller. **CVE ID: CVE-2024-42082**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.98					
Use of Uninitialized Resource	30-Jul-2024	7.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero Avoid potentially reusing uninitialized data **CVE ID: CVE-2024-42225**	https://git.kernel.org/stable/c/22ea2a7f0b64d323625950414a4496520fb33657, https://git.kernel.org/stable/c/64f86337ccfe77fe3be5a9356b0dabde23fbb074, https://git.kernel.org/stable/c/7f819a2f4fbc510e088b49c79addcf1734503578	O-LIN-LINU-020824/446
N/A	30-Jul-2024	4.1	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use	https://git.kernel.org/stable/c/23e4099bdc3c8381992f9eb975c7919 6d6755210, https://git.kernel.org/stable/c/28c8d274848feba552e95c5c2a7e3cfe8f15c534	O-LIN-LINU-020824/447

CVSS 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
			I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accomplish this by using kfree_sensitive for buffers that previously held the private key. **CVE ID: CVE-2024-42229**	, https://git.kernel.org/stable/c/71dd428615375e36523f4d4f7685ddd54113646d	
Affected Version(s): From (including) 5.16.10 Up to (excluding) 5.16.17					
Integer Overflow or Wraparound	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: prevent integer overflow in rndis_set_response() If "BufOffset" is very large the "BufOffset + 8" operation can have an integer overflow. **CVE ID: CVE-2022-48837**	https://git.kernel.org/stable/c/138d4f739b35dfb40438a0d5d7054965763bfbe7, https://git.kernel.org/stable/c/21829376268397f9fd2c35cfa9135937b6aa3a1e, https://git.kernel.org/stable/c/28bc0267399f42f987916a7174e2e32f0833cc65	O-LIN-LINU-020824/448
Affected Version(s): From (including) 5.16.13 Up to (excluding) 5.16.17					

CVSS 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
Loop with Unreachable Exit Condition ('Infinite Loop')	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iavf: Fix hang during reboot/shutdown Recent commit 974578017fc1 ("iavf: Add waiting so the port is initialized in remove") adds a wait-loop at the beginning of iavf_remove() to ensure that port initialization is finished prior unregistering net device. This causes a regression in reboot/shutdown scenario because in this case callback iavf_shutdown() is called and this callback detaches the device, makes it down if it is running and sets its state to __IAVF_REMOVE. Later shutdown callback of associated PF	https://git.kernel.org/stable/c/4477b9a4193b35eb3a8afd2adf2d42add2f88d57, https://git.kernel.org/stable/c/80974bb730270199c6fcb189af04d5945b87e813, https://git.kernel.org/stable/c/b04683ff8f0823b869c219c78ba0d974bddea0b5	O-LIN-LINU-020824/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver (e.g. ice_shutdown) is called. That callback calls among other things sriov_disable() that calls indirectly iavf_remove() (see stack trace below). As the adapter state is already __IAVF_REMOVE then the mentioned loop is end-less and shutdown process hangs. The patch fixes this by checking adapter's state at the beginning of iavf_remove() and skips the rest of the function if the adapter is already in remove state (shutdown is in progress). Reproducer: 1. Create VF on PF driven by ice or i40e driver 2. Ensure that the VF is bound to iavf driver 3. Reboot		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[52625.981294] sysrq: SysRq : Show Blocked State [52625.988377] task:reboot state:D stack: 0 pid:17359 ppid: 1 f2 [52625.996732] Call Trace: [52625.999187] __schedule+0x2d1/0x830 [52626.007400] schedule+0x35/0xa0 [52626.010545] schedule_hrtimeout_range_clock+0x83/0x100 [52626.020046] usleep_range+0x5b/0x80 [52626.023540] iavf_remove+0x63/0x5b0 [iavf] [52626.027645] pci_device_remove+0x3b/0xc0 [52626.031572] device_release_driver_internal+0x103/0x1f0 [52626.036805] pci_stop_bus_device+0x72/0xa0 [52626.040904] pci_stop_and_remove_bus_device+0xe/0x20		

CVSS 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
			[52626.045870] pci_iov_remove_virtfn+0xba/0x120 [52626.050232] sriov_disable+0x2f/0xe0 [52626.053813] ice_free_vfs+0x7c/0x340 [ice] [52626.057946] ice_remove+0x220/0x240 [ice] [52626.061967] ice_shutdown+0x16/0x50 [ice] [52626.065987] pci_device_shutdown+0x34/0x60 [52626.070086] device_shutdown+0x165/0x1c5 [52626.074011] kernel_restart+0xe/0x30 [52626.077593] __do_sys_reboot+0x1d2/0x210 [52626.093815] do_syscall_64+0x5b/0x1a0 [52626.097483] entry_SYSCALL_64_after_hwframe+0x65/0xca **CVE ID: CVE-2022-48840**		
Affected Version(s): From (including) 5.4.1 Up to (excluding) 5.4.279					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf	https://git.kernel.org/stable/c/4c5dc3927e17489c1cae6f48c0d5e4acb4cae01f, https://git.kernel.org/stable/c/5e4ed38eb17eaca42de57d500cc0f9668d2b6abf, https://git.kernel.org/stable/c/a2a0ebff7fdeb2f66e29335adf64b9e457300dd4	O-LIN-LINU-020824/450

CVSS 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
			include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ___sys_recvmsg+0x18a/0x620 net/socket.c:2803 __sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730		

CVSS 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/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ___sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline]		

CVSS 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
			do_syscall_64+0xcf /0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 **CVE ID: CVE-2024-42076**		
Affected Version(s): From (including) 5.4.180 Up to (excluding) 5.4.187					
Integer Overflow or	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/138d4f739b35dfb40438a0d5d7	O-LIN-LINU-020824/451

CVSS 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
Wraparound			usb: gadget: rndis: prevent integer overflow in rndis_set_response() If "BufOffset" is very large the "BufOffset + 8" operation can have an integer overflow. **CVE ID: CVE-2022-48837**	054965763bfbe7, https://git.kernel.org/stable/c/218293762683 97f9fd2c35cfa9 135937b6aa3a1e, https://git.kernel.org/stable/c/28bc0267399f4 2f987916a7174 e2e32f0833cc65	
Affected Version(s): From (including) 5.4.187 Up to (excluding) 5.10.108					
N/A	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: usbtmc: Fix bug in pipe direction for control transfers The syzbot fuzzer reported a minor bug in the usbtmc driver: usb 5-1: BOGUS control dir, pipe 80001e80 doesn't match bRequestType 0 WARNING: CPU: 0 PID: 3813 at	https://git.kernel.org/stable/c/10a805334a11a cd547602d6c4c f540a0f6ab5c6e, https://git.kernel.org/stable/c/5f6a2d63c68c1 2cf61259df7c3 527a0e05dce952, https://git.kernel.org/stable/c/700a0715854c 1e79a7334172 4ce4f5bb01abc 016	O-LIN-LINU-020824/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/usb/core/urb.c:412 usb_submit_urb+0x13a5/0x1970 drivers/usb/core/urb.c:410 Modules linked in: CPU: 0 PID: 3813 Comm: syz-executor122 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #0 ... Call Trace: <TASK> usb_start_wait_urb+0x113/0x530 drivers/usb/core/message.c:58 usb_internal_control_msg drivers/usb/core/message.c:102 [inline] usb_control_msg+0x2a5/0x4b0 drivers/usb/core/message.c:153 usbtmc_ioctl_request drivers/usb/class/usbtmc.c:1947 [inline]		

CVSS 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 problem is that usbtmc_ioctl_request() uses usb_rcvctrlpipe() for all of its transfers, whether they are in or out. It's easy to fix. **CVE ID: CVE-2022-48834**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.106					
Use After Free	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: staging: gdm724x: fix use after free in gdm_lte_rx() The netif_rx_ni() function frees the skb so we can't dereference it to save the skb->len. **CVE ID: CVE-2022-48851**	https://git.kernel.org/stable/c/1fb9dd3787495b4deb0efe66c58306b65691a48f, https://git.kernel.org/stable/c/403e3afe241b62401de1f8629c9c6b9b3d69dbff, https://git.kernel.org/stable/c/48ecdf3e29a6e514e8196691589c7dfc6c4ac169	O-LIN-LINU-020824/453
Missing Release of Memory after Effective Lifetime	16-Jul-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: sctp: fix kernel-infoleak for SCTP sockets	https://git.kernel.org/stable/c/1502f15b9f29c41883a6139f2923523873282a83, https://git.kernel.org/stable/c/2d8fa3fdf4542a2174a72d92018f488d65d848c5,	O-LIN-LINU-020824/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syzbot reported a kernel infoleak [1] of 4 bytes. After analysis, it turned out r->idiag_expires is not initialized if inet_sctp_diag_fill() calls inet_diag_msg_common_fill() Make sure to clear idiag_timer/idiag_retrans/idiag_expires and let inet_diag_msg_sctpasoc_fill() fill them again if needed. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline] BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:154 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x6e	https://git.kernel.org/stable/c/3fc0fd724d199e061432b66a8d85b7d48fe485f7	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f/0x25a0 lib/iov_iter.c:668 instrument_copy_to_user include/linux/instrumented.h:121 [inline] copyout lib/iov_iter.c:154 [inline] _copy_to_iter+0x6ef/0x25a0 lib/iov_iter.c:668 copy_to_iter include/linux/uio.h:162 [inline] simple_copy_to_iter+0xf3/0x140 net/core/datagram.c:519 __skb_datagram_iter+0x2d5/0x11b0 net/core/datagram.c:425 skb_copy_datagram_iter+0xdc/0x270 net/core/datagram.c:533 skb_copy_datagram_msg include/linux/skbuff.h:3696 [inline] netlink_recvmsg+0x669/0x1c80		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netlink/af_netlink.c:1977 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] __sys_recvfrom+0x795/0xa10 net/socket.c:2097 __do_sys_recvfrom net/socket.c:2115 [inline] __se_sys_recvfrom net/socket.c:2111 [inline] __x64_sys_recvfrom+0x19d/0x210 net/socket.c:2111 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae Uninit was created at: slab_post_alloc_hoo		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k mm/slab.h:737 [inline] slab_alloc_node mm/slub.c:3247 [inline] __kmalloc_node_track_caller+0xe0c/0x1510 mm/slub.c:4975 kmalloc_reserve net/core/skbuff.c:354 [inline] __alloc_skb+0x545/0xf90 net/core/skbuff.c:426 alloc_skb include/linux/skbuff.h:1158 [inline] netlink_dump+0x3e5/0x16c0 net/netlink/af_netlink.c:2248 __netlink_dump_start+0xcf8/0xe90 net/netlink/af_netlink.c:2373 netlink_dump_start include/linux/netlink.h:254 [inline] inet_diag_handler_cmd+0x2e7/0x400 net/ipv4/inet_diag.c:1341		

CVSS 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_diag_rcv_msg +0x24a/0x620 netlink_rcv_skb+0x 40c/0x7e0 net/netlink/af_netl ink.c:2494 sock_diag_rcv+0x6 3/0x80 net/core/sock_diag .c:277 netlink_unicast_ker nel net/netlink/af_netl ink.c:1317 [inline] netlink_unicast+0x 1093/0x1360 net/netlink/af_netl ink.c:1343 netlink_sendmsg+0 x14d9/0x1720 net/netlink/af_netl ink.c:1919 sock_sendmsg_nos ec net/socket.c:705 [inline] sock_sendmsg net/socket.c:725 [inline] sock_write_iter+0x 594/0x690 net/socket.c:1061		

CVSS 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
			do_iter_readv_writev+0xa7f/0xc70 do_iter_write+0x52c/0x1500 fs/read_write.c:851 vfs_writev fs/read_write.c:924 [inline] do_writev+0x645/0xe00 fs/read_write.c:967 __do_sys_writev fs/read_write.c:1040 [inline] __se_sys_writev fs/read_write.c:1037 [inline] __x64_sys_writev+0xe5/0x120 fs/read_write.c:1037 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x44/0xae		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bytes 68-71 of 2508 are uninitialized Memory access of size 2508 starts at ffff888114f9b000 Data copied to user address 00007f7fe09ff2e0 CPU: 1 PID: 3478 Comm: syz-executor306 Not tainted 5.17.0-rc4-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 **CVE ID: CVE-2022-48855**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Jul-2024	7	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix a race on command flush flow Fix a refcount use after free warning due to a race on command entry. Such race occurs when one of the	https://git.kernel.org/stable/c/0401bfb27a91d7bdd74b1635c1aae57cbb128da6, https://git.kernel.org/stable/c/063bd355595428750803d8736a9bb7c8db67d42d, https://git.kernel.org/stable/c/1a4017926eeea56c7540cc41b4	O-LIN-LINU-020824/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands releases its last refcount and frees its index and entry while another process running command flush flow takes refcount to this command entry. The process which handles commands flush may see this command as needed to be flushed if the other process released its refcount but didn't release the index yet. Fix it by adding the needed spin lock. It fixes the following warning trace: refcount_t: addition on 0; use-after-free. WARNING: CPU: 11 PID: 540311 at lib/refcount.c:25 refcount_warn_saturate+0x80/0xe0 ... RIP: 0010:refcount_warn_saturate+0x80/0xe0 ...	2106746ee8a0ee	

CVSS 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
			Call Trace: <TASK> mlx5_cmd_trigger_completions+0x293/0x340 [mlx5_core] mlx5_cmd_flush+0x3a/0xf0 [mlx5_core] enter_error_state+0x44/0x80 [mlx5_core] mlx5_fw_fatal_reporter_err_work+0x37/0xe0 [mlx5_core] process_one_work+0x1be/0x390 worker_thread+0x4d/0x3d0 ? rescuer_thread+0x350/0x350 kthread+0x141/0x160 ? set_kthread_struct+0x40/0x40 ret_from_fork+0x1f/0x30 </TASK>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48858		
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net-sysfs: add check for netdevice being present to speed_show When bringing down the netdevice or system shutdown, a panic can be triggered while accessing the sysfs path because the device is already removed. [755.549084] mlx5_core 0000:12:00.1: Shutdown was called [756.404455] mlx5_core 0000:12:00.0: Shutdown was called ... [757.937260] BUG: unable to handle kernel NULL pointer dereference at (null)	https://git.kernel.org/stable/c/081369ad088a76429984483b8a5f7e967a125aad, https://git.kernel.org/stable/c/3a79f380b3e10edf6caa9aac90163a5d7a282204, https://git.kernel.org/stable/c/4224cfd7fb6523f7a9d1c8bb91bb5df1e38eb624	O-LIN-LINU-020824/456

CVSS 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
			[758.031397] IP: [<ffffffff8ee11acb>] dma_pool_alloc+0x1ab/0x280 crash> bt ... PID: 12649 TASK: ffff8924108f2100 CPU: 1 COMMAND: "amsd" ... #9 [ffff89240e1a38b0] page_fault at ffffffff8f38c778 [exception RIP: dma_pool_alloc+0x1ab] RIP: ffffffff8ee11acb RSP: ffff89240e1a3968 RFLAGS: 00010046 RAX: 0000000000000246 RBX: ffff89243d874100 RCX: 0000000000001000 RDX: 0000000000000000 RSI: 0000000000000246 RDI: ffff89243d874090		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: ffff89240e1a39c0 R8: 000000000001f080 R9: ffff8905ffc03c00 R10: ffffffffc04680d4 R11: ffffffff8edde9fd R12: 00000000000080d0 R13: ffff89243d874090 R14: ffff89243d874080 R15: 0000000000000000 ORIG_RAX: ffffffffffffffff CS: 0010 SS: 0018 #10 [ffff89240e1a39c8] mlx5_alloc_cmd_msg at ffffffffc04680f3 [mlx5_core] #11 [ffff89240e1a3a18] cmd_exec at ffffffffc046ad62 [mlx5_core] #12 [ffff89240e1a3ab8] mlx5_cmd_exec at ffffffffc046b4fb [mlx5_core] #13 [ffff89240e1a3ae8] mlx5_core_access_reg at		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffffffffc0475434 [mlx5_core] #14 [ffff89240e1a3b40] mlx5e_get_fec_caps at ffffffffc04a7348 [mlx5_core] #15 [ffff89240e1a3bb0] get_fec_supported_advertised at ffffffffc04992bf [mlx5_core] #16 [ffff89240e1a3c08] mlx5e_get_link_ksettings at ffffffffc049ab36 [mlx5_core] #17 [ffff89240e1a3ce8] __ethtool_get_link_ksettings at ffffffff8f25db46 #18 [ffff89240e1a3d48] speed_show at ffffffff8f277208 #19 [ffff89240e1a3dd8] dev_attr_show at ffffffff8f0b70e3 #20 [ffff89240e1a3df8] sysfs_kf_seq_show at ffffffff8eedbedf #21 [ffff89240e1a3e18]		

CVSS 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
			kernfs_seq_show at ffffffff8eeda596 #22 [ffff89240e1a3e28] seq_read at ffffffff8ee76d10 #23 [ffff89240e1a3e98] kernfs_fop_read at ffffffff8eedaef5 #24 [ffff89240e1a3ed8] vfs_read at ffffffff8ee4e3ff #25 [ffff89240e1a3f08] sys_read at ffffffff8ee4f27f #26 [ffff89240e1a3f50] system_call_fastpath at ffffffff8f395f92 crash> net_device.state ffff89443b0c0000 state = 0x5 (__LINK_STATE_START| __LINK_STATE_NOCARRIER) To prevent this scenario, we also make sure that the netdevice is present. **CVE ID: CVE-2022-48850**		

CVSS 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	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gianfar: ethtool: Fix refcount leak in gfar_get_ts_info The of_find_compatible_node() function returns a node pointer with refcount incremented, We should use of_node_put() on it when done Add the missing of_node_put() to release the refcount. **CVE ID: CVE-2022-48856**	https://git.kernel.org/stable/c/0e1b9a2078e07fb1e6e91bf8badfd89ecab1e848, https://git.kernel.org/stable/c/21044e679ed535345042d2023f7df0ca8e897e2a, https://git.kernel.org/stable/c/2ac5b58e645c66932438bb021cb5b52097ce70b0	O-LIN-LINU-020824/457
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: NFC: port100: fix use-after-free in port100_send_complete Syzbot reported UAF in port100_send_complete(). The root case is in	https://git.kernel.org/stable/c/0e721b8f2ee5e11376dd55363f9ccb539d754b8a, https://git.kernel.org/stable/c/205c4ec78e71cbf561794e6043da80e7bae6790f, https://git.kernel.org/stable/c/2b1c85f56512d49e43bc53741f	O-LIN-LINU-020824/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing usb_kill_urb() calls on error handling path of ->probe function. port100_send_complete() accesses devm allocated memory which will be freed on probe failure. We should kill this urbs before returning an error from probe function to prevent reported use-after-free Fail log: BUG: KASAN: use-after-free in port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 Read of size 1 at addr ffff88801bb59540 by task ksoftirqd/2/26 ... Call Trace: <TASK>	ce2f508cd90029	

CVSS 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
			__dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 port100_send_complete+0x16e/0x1a0 drivers/nfc/port100.c:935 __usb_hcd_giveback_urb+0x2b0/0x5c0 drivers/usb/core/hcd.c:1670 ... Allocated by task 1255: kasan_save_stack+		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x1e/0x40 mm/kasan/common.c:38 kasan_set_track mm/kasan/common.c:45 [inline] set_alloc_info mm/kasan/common.c:436 [inline] ___kasan_kmalloc mm/kasan/common.c:515 [inline] ___kasan_kmalloc mm/kasan/common.c:474 [inline] __kasan_kmalloc+0xa6/0xd0 mm/kasan/common.c:524 alloc_dr drivers/base/devres.c:116 [inline] devm_kmalloc+0x96/0x1d0 drivers/base/devres.c:823 devm_kzalloc include/linux/device.h:209 [inline] port100_probe+0x8a/0x1320 drivers/nfc/port100.c:1502 Freed by task 1255: kasan_save_stack+		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x1e/0x40 mm/kasan/common.c:38 kasan_set_track+0x21/0x30 mm/kasan/common.c:45 kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370 ___kasan_slab_free mm/kasan/common.c:366 [inline] ___kasan_slab_free+0xff/0x140 mm/kasan/common.c:328 kasan_slab_free include/linux/kasan.h:236 [inline] __cache_free mm/slab.c:3437 [inline] kfree+0xf8/0x2b0 mm/slab.c:3794 release_nodes+0x112/0x1a0 drivers/base/devres.c:501 devres_release_all+0x114/0x190 drivers/base/devres.c:530 really_probe+0x62		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6/0xcc0 drivers/base/dd.c:670 **CVE ID: CVE-2022-48857**		
Missing Release of Memory after Effective Lifetime	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ethernet: Fix error handling in xemaclite_of_probe This node pointer is returned by of_parse_phandle() with refcount incremented in this function. Calling of_node_put() to avoid the refcount leak. As the remove function do. **CVE ID: CVE-2022-48860**	https://git.kernel.org/stable/c/1852854ee349881efb78ccdbbb237838975902e4, https://git.kernel.org/stable/c/5e7c402892e189a7bc152b125e72261154aa585d, https://git.kernel.org/stable/c/669172ce976608b25a2f76f3c65d47f042d125c9	O-LIN-LINU-020824/459
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.107					
NULL Pointer Dereference	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vrr: Set VRR capable prop only if it is attached to connector	https://git.kernel.org/stable/c/0ba557d330946c23559aaea2d51ea649fdeca98a, https://git.kernel.org/stable/c/3534c5c005ef99a1804ed50b8a72cdae254cabb5,	O-LIN-LINU-020824/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VRR capable property is not attached by default to the connector It is attached only if VRR is supported. So if the driver tries to call drm core set prop function without it being attached that causes NULL dereference. **CVE ID: CVE-2022-48843**	https://git.kernel.org/stable/c/62929726ef0ec72cbbe9440c5d125d4278b99894	
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: smp: fill in sibling and core maps earlier After enabling CONFIG_SCHED_CORE (landed during 5.14 cycle), 2-core 2-thread-per-core interAptiv (CPS-driven) started emitting the following: [0.025698] CPU1 revision is: 0001a120 (MIPS interAptiv (multi))	https://git.kernel.org/stable/c/32813321f18d5432cec1b1a6ecc964f9ea26d565, https://git.kernel.org/stable/c/56eaacb8137ba2071ce48d4e3d91979270e139a7, https://git.kernel.org/stable/c/7315f8538db009605ffba00370678142ef00ac98	O-LIN-LINU-020824/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.048183] ----------[cut here]---------- [0.048187] WARNING: CPU: 1 PID: 0 at kernel/sched/core.c:6025 sched_core_cpu_starting+0x198/0x240 [0.048220] Modules linked in: [0.048233] CPU: 1 PID: 0 Comm: swapper/1 Not tainted 5.17.0-rc3+ #35 b7b319f24073fd9a3c2aa7ad15fb7993eec0b26f [0.048247] Stack : 817f000000000004 327804c8810eb050 0000000000000004 0000000000000000 c314fdd1 [0.048278] 830cbd64819c0000 8180000081 7f0000 83070bf400000001 830cbd0800000000 [0.048307] 0000000000000000		

CVSS 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
			815fcbc4 00000000 00000000 00000000 00000000 00000000 [0.048334] 00000000 00000000 00000000 00000000 817f0000 00000000 00000000 817f6f34 [0.048361] 817f0000 818a3c00 817f0000 00000004 00000000 00000000 4dc33260 0018c933 [0.048389] ... [0.048396] Call Trace: [0.048399] [<8105a7bc>] show_stack+0x3c/0x140 [0.048424] [<8131c2a0>] dump_stack_lvl+0x60/0x80 [0.048440] [<8108b5c0>] __warn+0xc0/0xf4 [0.048454] [<8108b658>]		

CVSS 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
			warn_slowpath_fmt +0x64/0x10c [0.048467] [<810bd418>] sched_core_cpu_starting+0x198/0x240 [0.048483] [<810c6514>] sched_cpu_starting +0x14/0x80 [0.048497] [<8108c0f8>] cpuhp_invoke_callback_range+0x78/0x140 [0.048510] [<8108d914>] notify_cpu_starting +0x94/0x140 [0.048523] [<8106593c>] start_secondary+0xbc/0x280 [0.048539] [0.048543] ---[end trace 0000000000000000]--- [0.048636] Synchronize counters for CPU 1: done. ...for each but CPU 0/boot. Basic debug printks right before the mentioned line say:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0.048170] CPU: 1, smt_mask: So smt_mask, which is sibling mask obviously, is empty when entering the function. This is critical, as sched_core_cpu_starting() calculates core-scheduling parameters only once per CPU start, and it's crucial to have all the parameters filled in at that moment (at least it uses cpu_smt_mask() which in fact is `&cpu_sibling_map[cpu]` on MIPS). A bit of debugging led me to that set_cpu_sibling_map() performing the actual map calculation, was being invocated after notify_cpu_start(), and exactly the latter function starts CPU HP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			callback round (sched_core_cpu_starting() is basically a CPU HP callback). While the flow is same on ARM64 (maps after the notifier, although before calling set_cpu_online()), x86 started calculating sibling maps earlier than starting the CPU HP callbacks in Linux 4.14 (see [0] for the reference). Neither me nor my brief tests couldn't find any potential caveats in calculating the maps right after performing delay calibration, but the WARN splat is now gone. The very same debug prints now yield exactly what I expected from them: [0.048433] CPU: 1, smt_mask: 0-1 [0] https://git.kernel.o		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rg/pub/scm/linux/kernel/git/mips/linux.git/commit/?id=76ce7cfe35ef **CVE ID: CVE-2022-48845**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.108					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Input: aiptek - properly check endpoint type Syzbot reported warning in usb_submit_urb() which is caused by wrong endpoint type. There was a check for the number of endpoints, but not for the type of endpoint. Fix it by replacing old desc.bNumEndpoints check with usb_find_common_endpoints() helper for finding endpoints Fail log:	https://git.kernel.org/stable/c/35069e654bcab567ff8b9f0e68e1caf82c15dcd7, https://git.kernel.org/stable/c/5600f6986628dde888173409058847 4f54a540a8, https://git.kernel.org/stable/c/57277a8b5d881e02051ba9d7f6cb3f915c229821	O-LIN-LINU-020824/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usb 5-1: BOGUS urb xfer, pipe 1 != type 3 WARNING: CPU: 2 PID: 48 at drivers/usb/core/urb.c:502 usb_submit_urb+0xed2/0x18a0 drivers/usb/core/urb.c:502 Modules linked in: CPU: 2 PID: 48 Comm: kworker/2:2 Not tainted 5.17.0-rc6-syzkaller-00226-g07ebd38a0da2 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Workqueue: usb_hub_wq hub_event ... Call Trace: <TASK> aiptek_open+0xd5/0x130 drivers/input/tablet/aiptek.c:830 input_open_device+0x1bb/0x320 drivers/input/input.c:629		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kbd_connect+0xfe/0x160 drivers/tty/vt/keyboard.c:1593 **CVE ID: CVE-2022-48836**		
Use After Free	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: Fix use-after-free bug by not setting udc->dev.driver The syzbot fuzzer found a use-after-free bug: BUG: KASAN: use-after-free in dev_uevent+0x712/0x780 drivers/base/core.c:2320 Read of size 8 at addr ffff88802b934098 by task udevd/3689 CPU: 2 PID: 3689 Comm: udevd Not tainted 5.17.0-rc4-syzkaller-00229-g4f12b742eb2b #0 Hardware name: QEMU Standard PC	https://git.kernel.org/stable/c/00bdd9bf1ac6d401ad926d3d8df41b9f1399f646, https://git.kernel.org/stable/c/16b1941eac2bd499f065a6739a40ce0011a3d740, https://git.kernel.org/stable/c/2015c23610cd0efadaeca4d3a8d1dae9a45aa35a	O-LIN-LINU-020824/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Q35 + ICH9, 2009), BIOS 1.14.0-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x303 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 dev_uevent+0x712/0x780 drivers/base/core.c:2320 uevent_show+0x1b8/0x380 drivers/base/core.c:2391 dev_attr_show+0x4b/0x90		

CVSS 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

			drivers/base/core.c:2094
			
			Although the bug manifested in the driver core, the real cause was a
			race with the gadget core. dev_uevent() does:
			
			if (dev->driver)
			
			add_uevent_var(env, "DRIVER=%s", dev->driver->name);
			
			and between the test and the dereference of dev->driver, the gadget
			core sets dev->driver to NULL.
			
			The race wouldn't occur if the gadget core registered its devices on
			a real bus, using the standard synchronization techniques of the
			driver core. However, it's not necessary to make such a large change		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in order to fix this bug; all we need to do is make sure that udc->dev.driver is always NULL. In fact, there is no reason for udc->dev.driver ever to be set to anything, let alone to the value it currently gets: the address of the gadget's driver. After all, a gadget driver only knows how to manage a gadget, not how to manage a UDC. This patch simply removes the statements in the gadget core that touch udc->dev.driver. **CVE ID: CVE-2022-48838**		
Out-of-bounds Read	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix slab-out-of-bounds access in packet_recvmsg()	https://git.kernel.org/stable/c/268dcf1f7b3193bc446ec3d14e08a240e9561e4d, https://git.kernel.org/stable/c/70b7b3c055fd4a464da8da55ff4c1f84269f9b0	O-LIN-LINU-020824/464

CVSS 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
			syzbot found that when an AF_PACKET socket is using PACKET_COPY_THRESH and mmap operations, tpacket_rcv() is queueing skbs with garbage in skb->cb[], triggering a too big copy [1] Presumably, users of af_packet using mmap() already gets correct metadata from the mapped buffer, we can simply make sure to clear 12 bytes that might be copied to user space later. BUG: KASAN: stack-out-of-bounds in memcpy include/linux/fortify-string.h:225 [inline] BUG: KASAN: stack-out-of-bounds in packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 Write of size 165 at addr	2, https://git.kernel.org/stable/c/a055f5f2841f7522b44a2b1eccb1951b4b03d51a	

CVSS 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
			ffffc9000385fb78 by task syz-executor233/3631 CPU: 0 PID: 3631 Comm: syz-executor233 Not tainted 5.17.0-rc7-syzkaller-02396-g0b3660695e80 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0xf/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/kasan/report.c:459 check_region_inline mm/kasan/generic.c:183 [inline] kasan_check_range+0x13d/0x180 mm/kasan/generic.c:189 memcpy+0x39/0x60 mm/kasan/shadow.c:66 memcpy include/linux/fortify-string.h:225 [inline] packet_recvmsg+0x56c/0x1150 net/packet/af_packet.c:3489 sock_recvmsg_nosec net/socket.c:948 [inline] sock_recvmsg net/socket.c:966 [inline] sock_recvmsg net/socket.c:962 [inline] ___sys_recvmsg+0x2c4/0x600 net/socket.c:2632 ___sys_recvmsg+0x		

CVSS 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
			127/0x200 net/socket.c:2674 __sys_recvmsg+0xe2/0x1a0 net/socket.c:2704 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fdfd5954c29 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 41 15 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 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffcf8e71e48 EFLAGS: 00000246 ORIG_RAX: 000000000000002f RAX: ffffffffffffffda RBX:		

CVSS 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
			0000000000000003 RCX: 00007fdfd5954c29 RDX: 0000000000000000 RSI: 0000000020000500 RDI: 0000000000000005 RBP: 0000000000000000 R08: 000000000000000d R09: 000000000000000d R10: 0000000000000000 R11: 0000000000000246 R12: 00007ffcf8e71e60 R13: 00000000000f4240 R14: 000000000000c1ff R15: 00007ffcf8e71e54 </TASK> addr ffffc9000385fb78 is located in stack of task syz-executor233/3631 at offset 32 in frame: ___sys_recvmsg+0x0/0x600		

CVSS 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
			include/linux/uio.h :246 this frame has 1 object: [32, 160) 'addr' Memory state around the buggy address: ffffc9000385fa80: 00 04 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 ffffc9000385fb00: 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1 00 >ffffc9000385fb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 ^ ffffc9000385fc00: f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00 f1 ffffc9000385fc80: f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2 00 00 00 00 00 ========== **CVE ID: CVE-2022-48839**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.110					
N/A	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: swiotlb: fix info leak with DMA_FROM_DEVICE The problem I'm addressing was discovered by the LTP test covering cve-2018-1000204. A short description of what happens follows: 1) The test case issues a command code 00 (TEST UNIT READY) via the SG_IO interface with: dxfer_len == 524288, dxdfer_dir == SG_DXFER_FROM_DEV and a corresponding dxferp. The peculiar thing about this is that TUR is not reading from the device.	https://git.kernel.org/stable/c/270475d6d2410ec66e971bf181afe1958dad565e, https://git.kernel.org/stable/c/6bfc5377a210dbda2a237f16d94d1bd4f1335026, https://git.kernel.org/stable/c/7403f4118ab94be837ab9d770507537a8057bc63	O-LIN-LINU-020824/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2) In sg_start_req() the invocation of blk_rq_map_user() effectively bounces the user-space buffer. As if the device was to transfer into it. Since commit a45b599ad808 ("scsi: sg: allocate with __GFP_ZERO in sg_build_indirect()") we make sure this first bounce buffer is allocated with GFP_ZERO. 3) For the rest of the story we keep ignoring that we have a TUR, so the device won't touch the buffer we prepare as if the we had a DMA_FROM_DEVICE type of situation. My setup uses a virtio-scsi device and the buffer allocated by SG is mapped by the function virtqueue_add_split() which uses DMA_FROM_DEVIC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			E for the "in" sgs (here scatter-gather and not scsi generics). This mapping involves bouncing via the swiotlb (we need swiotlb to do virtio in protected guest like s390 Secure Execution, or AMD SEV). 4) When the SCSI TUR is done, we first copy back the content of the second (that is swiotlb) bounce buffer (which most likely contains some previous IO data), to the first bounce buffer, which contains all zeros. Then we copy back the content of the first bounce buffer to the user-space buffer. 5) The test case detects that the buffer, which it zero-initialized, ain't all zeros and fails.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			One can argue that this is an swiotlb problem, because without swiotlb we leak all zeros, and the swiotlb should be transparent in a sense that it does not affect the outcome (if all other participants are well behaved). Copying the content of the original buffer into the swiotlb buffer is the only way I can think of to make swiotlb transparent in such scenarios. So let's do just that if in doubt, but allow the driver to tell us that the whole mapped buffer is going to be overwritten, in which case we can preserve the old behavior and avoid the performance impact of the extra bounce. **CVE ID: CVE-2022-48853**		

CVSS 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
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.221					
Missing Release of Memory after Effective Lifetime	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers. **CVE ID: CVE-2024-42070**	https://git.kernel.org/stable/c/23752737c6a618e994f9a310ec2568881a6b49c4, https://git.kernel.org/stable/c/40188a25a9847dbeb7ec67517174a835a677752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b5153848bfa1c2980f	O-LIN-LINU-020824/466
Use of Uninitialized Resource	29-Jul-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/4c5dc3927e174	O-LIN-LINU-020824/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline]	89c1cae6f48c0d5e4acb4cae01f, https://git.kernel.org/stable/c/5e4ed38eb17eaca42de57d500cc0f9668d2b6abf, https://git.kernel.org/stable/c/a2a0ebff7fdeb2f66e29335adf64b9e457300dd4	

CVSS 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
			BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x36		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ___sys_recvmsg+0x18a/0x620 net/socket.c:2803 __sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline]		

CVSS 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_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277		

CVSS 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_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ___sys_sendmsg+0x877/0xb60 net/socket.c:2584 __sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0		

CVSS 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
			arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 **CVE ID: CVE-2024-42076**		
Affected Version(s): From (including) 5.7 Up to (excluding) 5.15.29					
Loop with Unreachable Exit Condition ('Infinite Loop')	16-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vhost: fix hung thread due to	https://git.kernel.org/stable/c/d9a747e6b6561280bf1791bb24c5e9e082193dad, https://git.kern	O-LIN-LINU-020824/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			erroneous iotlb entries In vhost_iotlb_add_range_ctx(), range size can overflow to 0 when start is 0 and last is ULONG_MAX. One instance where it can happen is when userspace sends an IOTLB message with iova=size=uaddr=0 (vhost_process_iotlb_msg). So, an entry with size = 0, start = 0, last = ULONG_MAX ends up in the iotlb. Next time a packet is sent, iotlb_access_ok() loops indefinitely due to that erroneous entry. Call Trace: <TASK> iotlb_access_ok+0x21b/0x3e0 drivers/vhost/vhost.c:1340 vq_meta_prefetch+0xbc/0x280	el.org/stable/c/e2ae38cf3d91837a493cb2093c87700ff3cbe667, https://git.kernel.org/stable/c/f8d88e86e90ea1002226d7ac2430152bfea003d1	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/vhost/vhost.c:1366 vhost_transport_do_send_pkt+0xe0/0xfd0 drivers/vhost/vsock.c:104 vhost_worker+0x23d/0x3d0 drivers/vhost/vhost.c:372 kthread+0x2e9/0x3a0 kernel/kthread.c:377 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:295 </TASK> Reported by syzbot at: https://syzkaller.appspot.com/bug?extid=0abd373e2e50d704db87 To fix this, do two things: 1. Return -EINVAL in vhost_chr_write_iter() when userspace asks to map		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a range with size 0. 2. Fix vhost_iotlb_add_range_ctx() to handle the range [0, ULONG_MAX] by splitting it into two entries. **CVE ID: CVE-2022-48862**		
Affected Version(s): From (including) 5.8 Up to (excluding) 5.10.106					
Out-of-bounds Write	16-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: watch_queue: Fix filter limit check In watch_queue_set_filter(), there are a couple of places where we check that the filter type value does not exceed what the type_filter bitmap can hold. One place calculates the number of bits by: if (tf[i].type >= sizeof(wfilter->type_filter) * 8) which is fine, but the second does:	https://git.kernel.org/stable/c/1b09f28f70a5046acd64138075ae3f095238b045, https://git.kernel.org/stable/c/648895da69ced90ca770fd941c3d9479a9d72c16, https://git.kernel.org/stable/c/b36588ebbcef74583824c08352e75838d6fb4ff2	O-LIN-LINU-020824/469

CVSS 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 (tf[i].type >= sizeof(wfilter->type_filter) * BITS_PER_LONG) which is not. This can lead to a couple of out-of-bounds writes due to a too-large type: (1) __set_bit() on wfilter->type_filter (2) Writing more elements in wfilter->filters[] than we allocated. Fix this by just using the proper WATCH_TYPE__NR instead, which is the number of types we actually know about. The bug may cause an oops looking something like: BUG: KASAN: slab-out-of-bounds in watch_queue_set_filter+0x659/0x740 Write of size 4 at addr ffff88800d2c66bc		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by task watch_queue_oob/611 ... Call Trace: <TASK> dump_stack_lvl+0x45/0x59 print_address_description.constprop.0+0x1f/0x150 ... kasan_report.cold+0x7f/0x11b ... watch_queue_set_filter+0x659/0x740 ... __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae Allocated by task 611: kasan_save_stack+0x1e/0x40		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kasan_kmalloc+0x81/0xa0 watch_queue_set_filter+0x23a/0x740 __x64_sys_ioctl+0x127/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae The buggy address belongs to the object at ffff88800d2c66a0 which belongs to the cache kmalloc-32 of size 32 The buggy address is located 28 bytes inside of 32-byte region [ffff88800d2c66a0, ffff88800d2c66c0) **CVE ID: CVE-2022-48847**		
Affected Version(s): From (including) 5.8 Up to (excluding) 6.1.97					
Allocation of Resources Without Limits or Throttling	17-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/47416c852f2a04d348ea66ee451cbdcf8119f225, https://git.kern	O-LIN-LINU-020824/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf: Fix overrunning reservations in ringbuf The BPF ring buffer internally is implemented as a power-of-2 sized circular buffer, with two logical and ever-increasing counters: consumer_pos is the consumer counter to show which logical position the consumer consumed the data, and producer_pos which is the producer counter denoting the amount of data reserved by all producers. Each time a record is reserved, the producer that "owns" the record will successfully advance producer counter. In user space each time a record is	el.org/stable/c/511804ab701c0503b72eac08217eabfd366ba069, https://git.kernel.org/stable/c/cfa1a2329a691ffd991fcf7248a57d752e712881	

CVSS 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
			read, the consumer of the data advanced the consumer counter once it finished processing. Both counters are stored in separate pages so that from user space, the producer counter is read-only and the consumer counter is read-write. One aspect that simplifies and thus speeds up the implementation of both producers and consumers is how the data area is mapped twice contiguously back-to-back in the virtual memory, allowing to not take any special measures for samples that have to wrap around at the end of the circular buffer data area, because the next page after the last data page would be first data page		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			again, and thus the sample will still appear completely contiguous in virtual memory. Each record has a struct bpf_ringbuf_hdr { u32 len; u32 pg_off; } header for book-keeping the length and offset, and is inaccessible to the BPF program. Helpers like bpf_ringbuf_reserve() return `(void *)hdr + BPF_RINGBUF_HDR_SZ` for the BPF program to use. Bing-Jhong and Muhammad reported that it is however possible to make a second allocated memory chunk overlapping with the first chunk and as a result, the BPF program is now able to edit first chunk's header.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For example, consider the creation of a BPF_MAP_TYPE_RINGBUF map with size of 0x4000. Next, the consumer_pos is modified to 0x3000 /before/ a call to bpf_ringbuf_reserve() is made. This will allocate a chunk A, which is in [0x0,0x3008], and the BPF program is able to edit [0x8,0x3008]. Now, lets allocate a chunk B with size 0x3000. This will succeed because consumer_pos was edited ahead of time to pass the `new_prod_pos - cons_pos > rb->mask` check. Chunk B will be in range [0x3008,0x6010], and the BPF program is able to edit [0x3010,0x6010]. Due to the ring buffer memory layout mentioned		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, the ranges [0x0,0x4000] and [0x4000,0x8000] point to the same data pages. This means that chunk B at [0x4000,0x4008] is chunk A's header. bpf_ringbuf_submit() / bpf_ringbuf_discard() use the header's pg_off to then locate the bpf_ringbuf itself via bpf_ringbuf_restore_from_rec(). Once chunk B modified chunk A's header, then bpf_ringbuf_commit() refers to the wrong page and could cause a crash. Fix it by calculating the oldest pending_pos and check whether the range from the oldest outstanding record to the newest would span beyond the ring buffer size. If that is the case, then reject		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the request. We've tested with the ring buffer benchmark in BPF selftests (./benchs/run_bench_ringbufs.sh) before/after the fix and while it seems a bit slower on some benchmarks, it is still not significantly enough to matter. **CVE ID: CVE-2024-41009**		
Affected Version(s): From (including) 5.9 Up to (excluding) 6.1.98					
N/A	30-Jul-2024	4.4	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with kexec kexec on pseries disables AIL (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can execute scv instructions after AIL is	https://git.kernel.org/stable/c/21a741eb75f80397e5f7d3739e24d7d75e619011, https://git.kernel.org/stable/c/8c6506616386ce37e59b2745fc481c6713fae4f3, https://git.kernel.org/stable/c/c550679d604798d9fed8a5b2bb5693448a25407c	O-LIN-LINU-020824/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to disable AIL after other CPUs have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head code probably couldn't easily deal with implementing such high addresses so it was just decided not to support that interrupt at all. **CVE ID: CVE-2024-42230**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.97					
Use After Free	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_buffers: Fix memory corruptions on	https://git.kernel.org/stable/c/942901e0fc74ad4b7992ef7ca9336e68d5fd6d36, https://git.kernel.org/stable/c/bf8781ede7bd9a37c0fcabca789	O-LIN-LINU-020824/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Spectrum-4 systems The following two shared buffer operations make use of the Shared Buffer Status Register (SBSR): # devlink sb occupancy snapshot pci/0000:01:00.0 # devlink sb occupancy clearmax pci/0000:01:00.0 The register has two masks of 256 bits to denote on which ingress / egress ports the register should operate on. Spectrum-4 has more than 256 ports, so the register was extended by cited commit with a new 'port_page' field. However, when filling the register's payload, the driver specifies the	76e61300b5a1a, https://git.kernel.org/stable/c/bfa86a96912faa0b6142a918db88cc0c738a769e	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ports as absolute numbers and not relative to the first port of the port page, resulting in memory corruptions [1]. Fix by specifying the ports relative to the first port of the port page. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 Read of size 1 at addr ffff8881068cb00f by task devlink/1566 [...] Call Trace: <TASK> dump_stack_lvl+0xc6/0x120 print_report+0xce/0x670 kasan_report+0xd7/0x110 mlxsw_sp_sb_occ_s		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			napshot+0xb6d/0xbc0 mlxsw_devlink_sb_occ_snapshot+0x75/0xb0 devlink_nl_sb_occ_snapshot_doit+0x1f9/0x2a0 genl_family_rcv_msg_doit+0x20c/0x300 genl_rcv_msg+0x567/0x800 netlink_rcv_skb+0x170/0x450 genl_rcv+0x2d/0x40 netlink_unicast+0x547/0x830 netlink_sendmsg+0x8d4/0xdb0 __sys_sendto+0x49b/0x510 __x64_sys_sendto+0xe5/0x1c0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_		

CVSS 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
			after_hwframe+0x77/0x7f [...] Allocated by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 copy_verifier_state+0xbc2/0xfb0 do_check_common+0x2c51/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

CVSS 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
			Freed by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 poison_slab_object+0x109/0x170 __kasan_slab_free+0x14/0x30 kfree+0xca/0x2b0 free_verifier_state+0xce/0x270 do_check_common+0x4828/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0		

CVSS 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+0x77/0x7f **CVE ID: CVE-2024-42073**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.37					
Allocation of Resources Without Limits or Throttling	17-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix overrunning reservations in ringbuf The BPF ring buffer internally is implemented as a power-of-2 sized circular buffer, with two logical and ever-increasing counters: consumer_pos is the consumer counter to show which logical position the consumer consumed the data, and producer_pos which is the producer counter denoting the amount of	https://git.kernel.org/stable/c/47416c852f2a04d348ea66ee451cbdcf8119f225, https://git.kernel.org/stable/c/511804ab701c0503b72eac08217eabfd366ba069, https://git.kernel.org/stable/c/cfa1a2329a691ffd991fcf7248a57d752e712881	O-LIN-LINU-020824/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data reserved by all producers. Each time a record is reserved, the producer that "owns" the record will successfully advance producer counter. In user space each time a record is read, the consumer of the data advanced the consumer counter once it finished processing. Both counters are stored in separate pages so that from user space, the producer counter is read-only and the consumer counter is read-write. One aspect that simplifies and thus speeds up the implementation of both producers and consumers is how the data area is mapped twice contiguously back-to-back in the virtual memory, allowing to not take		

CVSS 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
			any special measures for samples that have to wrap around at the end of the circular buffer data area, because the next page after the last data page would be first data page again, and thus the sample will still appear completely contiguous in virtual memory. Each record has a struct bpf_ringbuf_hdr { u32 len; u32 pg_off; } header for book-keeping the length and offset, and is inaccessible to the BPF program. Helpers like bpf_ringbuf_reserve() return `(void *)hdr + BPF_RINGBUF_HDR_SZ` for the BPF program to use. Bing-Jhong and Muhammad reported that it is however		

CVSS 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
			possible to make a second allocated memory chunk overlapping with the first chunk and as a result, the BPF program is now able to edit first chunk's header. For example, consider the creation of a BPF_MAP_TYPE_RINGBUF map with size of 0x4000. Next, the consumer_pos is modified to 0x3000 /before/ a call to bpf_ringbuf_reserve() is made. This will allocate a chunk A, which is in [0x0,0x3008], and the BPF program is able to edit [0x8,0x3008]. Now, lets allocate a chunk B with size 0x3000. This will succeed because consumer_pos was edited ahead of time to pass the `new_prod_pos - cons_pos > rb->mask`		

CVSS 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. Chunk B will be in range [0x3008,0x6010], and the BPF program is able to edit [0x3010,0x6010]. Due to the ring buffer memory layout mentioned earlier, the ranges [0x0,0x4000] and [0x4000,0x8000] point to the same data pages. This means that chunk B at [0x4000,0x4008] is chunk A's header. bpf_ringbuf_submit() / bpf_ringbuf_discard() use the header's pg_off to then locate the bpf_ringbuf itself via bpf_ringbuf_restore_from_rec(). Once chunk B modified chunk A's header, then bpf_ringbuf_commit() refers to the wrong page and could cause a crash. Fix it by calculating the oldest pending_pos and		

CVSS 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 the range from the oldest outstanding record to the newest would span beyond the ring buffer size. If that is the case, then reject the request. We've tested with the ring buffer benchmark in BPF selftests (./benchs/run_bench_ringbufs.sh) before/after the fix and while it seems a bit slower on some benchmarks, it is still not significantly enough to matter. **CVE ID: CVE-2024-41009**		
Unchecked Return Value	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into account with bpf_prog_lock_ro() set_memory_ro() can fail, leaving	https://git.kernel.org/stable/c/05412471beba313ecded95aa17b25fe84bb2551a, https://git.kernel.org/stable/c/7d2cc63eca0c993c99d18893214abf8f85d566d8, https://git.kernel.org/stable/c/a359696856ca9	O-LIN-LINU-020824/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory unprotected. Check its return and take it into account as an error. **CVE ID: CVE-2024-42068**	409fb97655c5a8ef0f549cb6e03	
Missing Release of Memory after Effective Lifetime	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be	https://git.kernel.org/stable/c/23752737c6a618e994f9a310ec2568881a6b49c4, https://git.kernel.org/stable/c/40188a25a9847dbeb7ec67517174a835a677752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b5153848bfa1c2980f	O-LIN-LINU-020824/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leaked through the registers. **CVE ID: CVE-2024-42070**		
Use After Free	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_buffers: Fix memory corruptions on Spectrum-4 systems The following two shared buffer operations make use of the Shared Buffer Status Register (SBSR): # devlink sb occupancy snapshot pci/0000:01:00.0 # devlink sb occupancy clearmax pci/0000:01:00.0 The register has two masks of 256 bits to denote on which ingress / egress ports the register should operate on.	https://git.kernel.org/stable/c/942901e0fc74ad4b7992ef7ca9336e68d5fd6d36, https://git.kernel.org/stable/c/bf8781ede7bd9a37c0fcabca78976e61300b5a1a, https://git.kernel.org/stable/c/bfa86a96912faa0b6142a918db88cc0c738a769e	O-LIN-LINU-020824/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Spectrum-4 has more than 256 ports, so the register was extended by cited commit with a new 'port_page' field. However, when filling the register's payload, the driver specifies the ports as absolute numbers and not relative to the first port of the port page, resulting in memory corruptions [1]. Fix by specifying the ports relative to the first port of the port page. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 Read of size 1 at addr ffff8881068cb00f by task devlink/1566 [...] Call Trace: <TASK>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dump_stack_lvl+0xc6/0x120 print_report+0xce/0x670 kasan_report+0xd7/0x110 mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 mlxsw_devlink_sb_occ_snapshot+0x75/0xb0 devlink_nl_sb_occ_snapshot_doit+0x1f9/0x2a0 genl_family_rcv_msg_doit+0x20c/0x300 genl_rcv_msg+0x567/0x800 netlink_rcv_skb+0x170/0x450 genl_rcv+0x2d/0x40 netlink_unicast+0x547/0x830 netlink_sendmsg+0x8d4/0xdb0		

CVSS 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_sendto+0x49b/0x510 __x64_sys_sendto+0xe5/0x1c0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [...] Allocated by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 copy_verifier_state+0xbc2/0xfb0 do_check_common+0x2c51/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 poison_slab_object+0x109/0x170 __kasan_slab_free+0x14/0x30 kfree+0xca/0x2b0 free_verifier_state+0xce/0x270 do_check_common+0x4828/0xc7e0 bpf_check+0x5107/0x9960		

CVSS 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_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f **CVE ID: CVE-2024-42073**		
Use of Uninitialized Resource	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing	https://git.kernel.org/stable/c/4c5dc3927e17489c1cae6f48c0d5e4acb4cae01f, https://git.kernel.org/stable/c/5e4ed38eb17eaca42de57d500cc0f9668d2b6abf, https://git.kernel.org/stable/c/a2a0ebff7fdeb2f66e29335adf64b9e457300dd4	O-LIN-LINU-020824/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instr		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			umented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c4/0x340 net/socket.c:1068 ___sys_recvmsg+0x18a/0x620 net/socket.c:2803 __sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0		

CVSS 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
			arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_ps		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline]		

CVSS 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
			__do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg +0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b /0x3b50 arch/x86/include/ generated/asm/sy scalls_64.h:47 do_syscall_x64 arch/x86/entry/co mmon.c:52 [inline] do_syscall_64+0xcf /0x1e0 arch/x86/entry/co mmon.c:83 entry_SYSCALL_64_ after_hwframe+0x 77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c 0		

CVSS 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: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 **CVE ID: CVE-2024-42076**		
N/A	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can	https://git.kernel.org/stable/c/320273b5649bbcee87f9e65343077189699d2a7a, https://git.kernel.org/stable/c/331d1079d58206ff7dc5518185f800b412f89bc6, https://git.kernel.org/stable/c/9ea2d1c6789722d58ec191f14f9a02518d55b6b4	O-LIN-LINU-020824/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain arbitrary number of extents. Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by one of our customers on a heavily fragmented OCFS2 filesystem. To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2]		

CVSS 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 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_		

CVSS 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
			write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba **CVE ID: CVE-2024-42077**		
Out-of-bounds Write	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address access struct rdma_restrack_entry's kern_name was set to	https://git.kernel.org/stable/c/782bdaf9d01658281bc813f3f873e6258aa1fd8d, https://git.kernel.org/stable/c/8656ef8a9288d6c932654f8d3856dc4ab1cfc6b5, https://git.kernel.org/stable/c/8ac281d42337f	O-LIN-LINU-020824/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this rdma_restrack_entry, it would cause a invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one forgotten PD release in one of the ULPs. But it is not needed anymore, so delete them. **CVE ID: CVE-2024-42080**	36cf7061cf1ea094181b84bc1a9	
Allocation of Resources Without Limits or Throttling	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model().	https://git.kernel.org/stable/c/1095b8efbb13a6a5fa583ed373ee1ccab29da2d0, https://git.kernel.org/stable/c/14e51ea78b4ccacb7acb1346b9241bb790a2054c, https://git.kernel.org/stable/c/1d3e3b3aa2cbe9bc7db9a7f867	O-LIN-LINU-020824/480

CVSS 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 warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation. Thus, there is no sense in using WARN() to handle this error and it can be safely removed.	3a9fa6d2990d54	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_li		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ve+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Found by Linux Verification Center		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(linuxtesting.org) with syzkaller. **CVE ID: CVE-2024-42082**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.39					
Use of Uninitialized Resource	30-Jul-2024	7.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero Avoid potentially reusing uninitialized data **CVE ID: CVE-2024-42225**	https://git.kernel.org/stable/c/22ea2a7f0b64d323625950414a4496520fb33657, https://git.kernel.org/stable/c/64f86337ccfe77fe3be5a9356b0dabde23fbb074, https://git.kernel.org/stable/c/7f819a2f4fbc510e088b49c79addcf1734503578	O-LIN-LINU-020824/481
N/A	30-Jul-2024	4.1	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accomplish this by	https://git.kernel.org/stable/c/23e4099bdc3c8381992f9eb975c7919 6d6755210, https://git.kernel.org/stable/c/28c8d274848feba552e95c5c2a7e3cfe8f15c534, https://git.kernel.org/stable/c/71dd428615375e36523f4d4f7685ddd54113646d	O-LIN-LINU-020824/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using kfree_sensitive for buffers that previously held the private key. **CVE ID: CVE-2024-42229**		
Affected Version(s): From (including) 6.2 Up to (including) 6.6.39					
N/A	30-Jul-2024	4.4	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with kexec kexec on pseries disables AIL (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can execute scv instructions after AIL is disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to disable	https://git.kernel.org/stable/c/21a741eb75f80397e5f7d3739e24d7d75e619011, https://git.kernel.org/stable/c/8c6506616386ce37e59b2745fc481c6713fae4f3, https://git.kernel.org/stable/c/c550679d604798d9fed8a5b2bb5693448a25407c	O-LIN-LINU-020824/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AIL after other CPUs have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head code probably couldn't easily deal with implementing such high addresses so it was just decided not to support that interrupt at all. **CVE ID: CVE-2024-42230**		
Affected Version(s): From (including) 6.3 Up to (excluding) 6.6.37					
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix possible double free in error handling path When auxiliary_device_add() returns error and then calls auxiliary_device_uninit(), callback function adev_release	https://git.kernel.org/stable/c/1864b8224195d0e43ddb92a8151f54f6562090cc, https://git.kernel.org/stable/c/3243e64eb4d897c3eeb48b2a7221ab5a95e1282a, https://git.kernel.org/stable/c/ed45c0a0b662079d4c0e518014cc148c753979b4	O-LIN-LINU-020824/484

CVSS 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
			calls kfree(madev). We shouldn't call kfree(madev) again in the error handling path. Set 'madev' to NULL. **CVE ID: CVE-2024-42069**		
Affected Version(s): From (including) 6.6 Up to (excluding) 6.6.41					
Use After Free	17-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix too early release of tcx_entry Pedro Pinto and later independently also Hyunwoo Kim and Wongi Lee reported an issue that the tcx_entry can be released too early leading to a use after free (UAF) when an active old-style ingress or clsact qdisc with a shared tc block is later replaced by another ingress or clsact instance. Essentially, the sequence to trigger the UAF (one	https://git.kernel.org/stable/c/1cb6f0bae50441f4b4b32a28315853b279c7404e, https://git.kernel.org/stable/c/230bb13650b0f186f540500fd5f5f7096a822a2a, https://git.kernel.org/stable/c/f61ecf1bd5b562ebfd7d430ccb3161985 7e80857	O-LIN-LINU-020824/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example) can be as follows: 1. A network namespace is created 2. An ingress qdisc is created. This allocates a tcx_entry, and &tcx_entry->miniq is stored in the qdisc's miniqp->p_miniq. At the same time, a tcf block with index 1 is created. 3. chain0 is attached to the tcf block. chain0 must be connected to the block linked to the ingress qdisc to later reach the function tcf_chain0_head_change_cb_del() which triggers the UAF. 4. Create and graft a clsact qdisc. This causes the ingress qdisc created in step 1 to be removed, thus freeing the previously linked tcx_entry:		

CVSS 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
			rtnetlink_rcv_msg() => tc_modify_qdisc() => qdisc_create() => clsact_init() [a] => qdisc_graft() => qdisc_destroy() => __qdisc_destroy() => ingress_destroy() [b] => tcx_entry_free() => kfree_rcu() // tcx_entry freed 5. Finally, the network namespace is closed. This registers the cleanup_net worker, and during the process of releasing the remaining clsact qdisc, it accesses the tcx_entry that was already freed in step 4, causing the UAF to occur:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleanup_net() => ops_exit_list() => default_device_exit_batch() => unregister_netdevice_many() => unregister_netdevice_many_notify() => dev_shutdown() => qdisc_put() => clsact_destroy() [c] => tcf_block_put_ext() => tcf_chain0_head_change_cb_del() => tcf_chain_head_change_item() => clsact_chain_head_change() => mini_qdisc_pair_swap() // UAF There are also other variants, the gist is to add an ingress (or clsact)		

CVSS 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
			qdisc with a specific shared block, then to replace that qdisc, waiting for the tcx_entry kfree_rcu() to be executed and subsequently accessing the current active qdisc's miniq one way or another. The correct fix is to turn the miniq_active boolean into a counter. What can be observed, at step 2 above, the counter transitions from 0->1, at step [a] from 1->2 (in order for the miniq object to remain active during the replacement), then in [b] from 2->1 and finally [c] 1->0 with the eventual release. The reference counter in general ranges from [0,2] and it does not need to be atomic since all access to the counter is protected		

CVSS 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
			by the rtnl mutex. With this in place, there is no longer a UAF happening and the tcx_entry is freed at the correct time. **CVE ID: CVE-2024-41010**		
Affected Version(s): From (including) 6.6.1 Up to (excluding) 6.6.37					
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp: add a null check for chip_pdev structure When acp platform device creation is skipped, chip->chip_pdev value will remain NULL. Add NULL check for chip->chip_pdev structure in snd_acp_resume() function to avoid null pointer dereference. **CVE ID: CVE-2024-42074**	https://git.kernel.org/stable/c/98d919dfee1cc402ca29d45da642852d7c9a2301, https://git.kernel.org/stable/c/b0c39ae1cc86afe74aa2f6273ccb514f8d180cf6, https://git.kernel.org/stable/c/e158ed266fc1adfa456880fb6dabce2e5623843b	O-LIN-LINU-020824/486
Affected Version(s): From (including) 6.7 Up to (excluding) 6.9.10					
Use After Free	17-Jul-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/1cb6f0bae50441f4b4b32a2831	O-LIN-LINU-020824/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: bpf: Fix too early release of tcx_entry Pedro Pinto and later independently also Hyunwoo Kim and Wongi Lee reported an issue that the tcx_entry can be released too early leading to a use after free (UAF) when an active old-style ingress or clsact qdisc with a shared tc block is later replaced by another ingress or clsact instance. Essentially, the sequence to trigger the UAF (one example) can be as follows: 1. A network namespace is created 2. An ingress qdisc is created. This allocates a tcx_entry, and &tcx_entry->miniq is stored in	5853b279c7404e, https://git.kernel.org/stable/c/230bb13650b0f186f540500fd5f5f7096a822a2a, https://git.kernel.org/stable/c/f61ecf1bd5b562ebfd7d430ccb3161985 7e80857	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the qdisc's miniqp->p_miniq. At the same time, a tcf block with index 1 is created. 3. chain0 is attached to the tcf block. chain0 must be connected to the block linked to the ingress qdisc to later reach the function tcf_chain0_head_change_cb_del() which triggers the UAF. 4. Create and graft a clsact qdisc. This causes the ingress qdisc created in step 1 to be removed, thus freeing the previously linked tcx_entry: rtnetlink_rcv_msg() => tc_modify_qdisc() => qdisc_create() => clsact_init() [a] => qdisc_graft()		

CVSS 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
			=> qdisc_destroy() => __qdisc_destroy() => ingress_destroy() [b] => tcx_entry_free() => kfree_rcu() // tcx_entry freed 5. Finally, the network namespace is closed. This registers the cleanup_net worker, and during the process of releasing the remaining clsact qdisc, it accesses the tcx_entry that was already freed in step 4, causing the UAF to occur: cleanup_net() => ops_exit_list() => default_device_exit_batch() => unregister_netdevice_many()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			=> unregister_netdevice_many_notify() => dev_shutdown() => qdisc_put() => clsact_destroy() [c] => tcf_block_put_ext() => tcf_chain0_head_change_cb_del() => tcf_chain_head_change_item() => clsact_chain_head_change() => mini_qdisc_pair_swap() // UAF There are also other variants, the gist is to add an ingress (or clsact) qdisc with a specific shared block, then to replace that qdisc, waiting for the tcx_entry kfree_rcu() to be executed and subsequently accessing		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the current active qdisc's miniq one way or another. The correct fix is to turn the miniq_active boolean into a counter. What can be observed, at step 2 above, the counter transitions from 0->1, at step [a] from 1->2 (in order for the miniq object to remain active during the replacement), then in [b] from 2->1 and finally [c] 1->0 with the eventual release. The reference counter in general ranges from [0,2] and it does not need to be atomic since all access to the counter is protected by the rtnl mutex. With this in place, there is no longer a UAF happening and the tcx_entry is freed at the correct time.		

CVSS 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-2024-41010		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.9.8					
Allocation of Resources Without Limits or Throttling	17-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix overrunning reservations in ringbuf The BPF ring buffer internally is implemented as a power-of-2 sized circular buffer, with two logical and ever-increasing counters: consumer_pos is the consumer counter to show which logical position the consumer consumed the data, and producer_pos which is the producer counter denoting the amount of data reserved by all producers. Each time a record is reserved, the	https://git.kernel.org/stable/c/47416c852f2a04d348ea66ee451cbdcf8119f225, https://git.kernel.org/stable/c/511804ab701c0503b72eac08217eabfd366ba069, https://git.kernel.org/stable/c/cfa1a2329a691ffd991fcf7248a57d752e712881	O-LIN-LINU-020824/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			producer that "owns" the record will successfully advance producer counter. In user space each time a record is read, the consumer of the data advanced the consumer counter once it finished processing. Both counters are stored in separate pages so that from user space, the producer counter is read-only and the consumer counter is read-write. One aspect that simplifies and thus speeds up the implementation of both producers and consumers is how the data area is mapped twice contiguously back-to-back in the virtual memory, allowing to not take any special measures for samples that have to wrap around at the end		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the circular buffer data area, because the next page after the last data page would be first data page again, and thus the sample will still appear completely contiguous in virtual memory. Each record has a struct bpf_ringbuf_hdr { u32 len; u32 pg_off; } header for book-keeping the length and offset, and is inaccessible to the BPF program. Helpers like bpf_ringbuf_reserve() return `(void *)hdr + BPF_RINGBUF_HDR_SZ` for the BPF program to use. Bing-Jhong and Muhammad reported that it is however possible to make a second allocated memory chunk overlapping with the first		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chunk and as a result, the BPF program is now able to edit first chunk's header. For example, consider the creation of a BPF_MAP_TYPE_RINGBUF map with size of 0x4000. Next, the consumer_pos is modified to 0x3000 /before/ a call to bpf_ringbuf_reserve() is made. This will allocate a chunk A, which is in [0x0,0x3008], and the BPF program is able to edit [0x8,0x3008]. Now, lets allocate a chunk B with size 0x3000. This will succeed because consumer_pos was edited ahead of time to pass the `new_prod_pos - cons_pos > rb->mask` check. Chunk B will be in range [0x3008,0x6010], and the BPF program is able		

CVSS 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
			to edit [0x3010,0x6010]. Due to the ring buffer memory layout mentioned earlier, the ranges [0x0,0x4000] and [0x4000,0x8000] point to the same data pages. This means that chunk B at [0x4000,0x4008] is chunk A's header. bpf_ringbuf_submit() / bpf_ringbuf_discard() use the header's pg_off to then locate the bpf_ringbuf itself via bpf_ringbuf_restore_from_rec(). Once chunk B modified chunk A's header, then bpf_ringbuf_commit() refers to the wrong page and could cause a crash. Fix it by calculating the oldest pending_pos and check whether the range from the oldest outstanding record to the newest		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would span beyond the ring buffer size. If that is the case, then reject the request. We've tested with the ring buffer benchmark in BPF selftests (./benchs/run_bench_ringbufs.sh) before/after the fix and while it seems a bit slower on some benchmarks, it is still not significantly enough to matter. **CVE ID: CVE-2024-41009**		
Unchecked Return Value	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_rox() into account with bpf_jit_binary_lock_ro() set_memory_rox() can fail, leaving memory unprotected. Check return and bail out when	https://git.kernel.org/stable/c/044da7ae7afd4ef60806d73654a2e6a79aa4ed7a, https://git.kernel.org/stable/c/08f6c05feb1db21653e98ca84ea04ca032d014c7, https://git.kernel.org/stable/c/9fef36cad60d4226f9d06953cd56d1d2f9119730	O-LIN-LINU-020824/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf_jit_binary_lock_ro() returns an error. **CVE ID: CVE-2024-42067**		
Unchecked Return Value	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into account with bpf_prog_lock_ro() set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error. **CVE ID: CVE-2024-42068**	https://git.kernel.org/stable/c/05412471beba313ecded95aa17b25fe84bb2551a, https://git.kernel.org/stable/c/7d2cc63eca0c993c99d18893214abf8f85d566d8, https://git.kernel.org/stable/c/a359696856ca9409fb97655c5a8ef0f549cb6e03	O-LIN-LINU-020824/490
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix possible double free in error handling path When auxiliary_device_ad	https://git.kernel.org/stable/c/1864b8224195d0e43ddb92a8151f54f6562090cc, https://git.kernel.org/stable/c/3243e64eb4d897c3eeb48b2a7221ab5a95e1282a, https://git.kernel.org/stable/c/	O-LIN-LINU-020824/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d() returns error and then calls auxiliary_device_uninit(), callback function adev_release calls kfree(madev). We shouldn't call kfree(madev) again in the error handling path. Set 'madev' to NULL. **CVE ID: CVE-2024-42069**	ed45c0a0b662079d4c0e518014cc148c753979b4	
Missing Release of Memory after Effective Lifetime	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the	https://git.kernel.org/stable/c/23752737c6a618e994f9a310ec2568881a6b49c4, https://git.kernel.org/stable/c/40188a25a9847dbeb7ec67517174a835a777752f, https://git.kernel.org/stable/c/41a6375d48deaf7f730304b5153848bfa1c2980f	O-LIN-LINU-020824/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers. **CVE ID: CVE-2024-42070**		
Use After Free	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_buffers: Fix memory corruptions on Spectrum-4 systems The following two shared buffer operations make use of the Shared Buffer Status Register (SBSR): # devlink sb occupancy snapshot pci/0000:01:00.0 # devlink sb occupancy clearmax pci/0000:01:00.0	https://git.kernel.org/stable/c/942901e0fc74ad4b7992ef7ca9336e68d5fd6d36, https://git.kernel.org/stable/c/bf8781ede7bd9a37c0fcabca78976e61300b5a1a, https://git.kernel.org/stable/c/bfa86a96912faa0b6142a918db88cc0c738a769e	O-LIN-LINU-020824/493

CVSS 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 register has two masks of 256 bits to denote on which ingress / egress ports the register should operate on. Spectrum-4 has more than 256 ports, so the register was extended by cited commit with a new 'port_page' field. However, when filling the register's payload, the driver specifies the ports as absolute numbers and not relative to the first port of the port page, resulting in memory corruptions [1]. Fix by specifying the ports relative to the first port of the port page. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 Read of size 1 at addr		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff8881068cb00f by task devlink/1566 [...] Call Trace: <TASK> dump_stack_lvl+0xc6/0x120 print_report+0xce/0x670 kasan_report+0xd7/0x110 mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 mlxsw_devlink_sb_occ_snapshot+0x75/0xb0 devlink_nl_sb_occ_snapshot_doit+0x1f9/0x2a0 genl_family_rcv_msg_doit+0x20c/0x300 genl_rcv_msg+0x567/0x800 netlink_rcv_skb+0x170/0x450		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			genl_rcv+0x2d/0x40 netlink_unicast+0x547/0x830 netlink_sendmsg+0x8d4/0xdb0 __sys_sendto+0x49b/0x510 __x64_sys_sendto+0xe5/0x1c0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [...] Allocated by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 copy_verifier_state+0xbc2/0xfb0 do_check_common+0x2c51/0xc7e0		

CVSS 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_check+0x5107 /0x9960 bpf_prog_load+0xf 0e/0x2690 __sys_bpf+0x1a61/ 0x49d0 __x64_sys_bpf+0x7 d/0xc0 do_syscall_64+0xc1 /0x1d0 entry_SYSCALL_64_ after_hwframe+0x 77/0x7f Freed by task 1: kasan_save_stack+ 0x33/0x60 kasan_save_track+ 0x14/0x30 kasan_save_free_inf o+0x3b/0x60 poison_slab_object +0x109/0x170 __kasan_slab_free+ 0x14/0x30 kfree+0xca/0x2b0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free_verifier_state+0xce/0x270 do_check_common+0x4828/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f **CVE ID: CVE-2024-42073**		
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp: add a null check for chip_pdev structure When acp platform device creation is skipped, chip-	https://git.kernel.org/stable/c/98d919dfee1cc402ca29d45da642852d7c9a2301, https://git.kernel.org/stable/c/b0c39ae1cc86afe74aa2f6273ccb514f8d180cf6, https://git.kernel.org/stable/c/e158ed266fc1a	O-LIN-LINU-020824/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>chip_pdev value will remain NULL. Add NULL check for chip->chip_pdev structure in snd_acp_resume() function to avoid null pointer dereference. **CVE ID: CVE-2024-42074**	dfa456880fb6dabce2e5623843b	
Use of Uninitialized Resource	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in	https://git.kernel.org/stable/c/4c5dc3927e17489c1cae6f48c0d5e4acb4cae01f, https://git.kernel.org/stable/c/5e4ed38eb17eaca42de57d500cc0f9668d2b6abf, https://git.kernel.org/stable/c/a2a0ebff7fdeb2f66e29335adf64b9e457300dd4	O-LIN-LINU-020824/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ___sys_recvmsg+0x18a/0x620 net/socket.c:2803		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			___sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

CVSS 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
			Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/net/sock.h :1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg +0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ___sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline]		

CVSS 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
			__x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0		

CVSS 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
			Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 **CVE ID: CVE-2024-42076**		
N/A	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do often extend the	https://git.kernel.org/stable/c/320273b5649bbcee87f9e65343077189699d2a7a, https://git.kernel.org/stable/c/331d1079d58206ff7dc5518185f800b412f89bc6, https://git.kernel.org/stable/c/9ea2d1c6789722d58ec191f14f9a02518d55b6b4	O-LIN-LINU-020824/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 filesystem.		

CVSS 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
			To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2] #4 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_write at ffffffff8c1dcf14 #15 __generic_file_write		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba **CVE ID: CVE-2024-42077**		
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix NULL pointer dereference in gfs2_log_flush In gfs2_jindex_free(), set sdp->sd_jdesc to NULL under the log flush lock to provide exclusion against gfs2_log_flush().	https://git.kernel.org/stable/c/3429ef5f50909cee9e498c50f0c499b9397116ce, https://git.kernel.org/stable/c/35264909e9d1973ab9aaa2a1b07cda70f12bb828, https://git.kernel.org/stable/c/f54f9d5368a4e92ede7dd078a62788dae3a7c6ef	O-LIN-LINU-020824/497

CVSS 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_log_flush(), check if sdp->sd_jdesc is non-NULL before dereferencing it. Otherwise, we could run into a NULL pointer dereference when outstanding glock work races with an unmount (glock_work_func -> run_queue -> do_xmote -> inode_go_sync -> gfs2_log_flush). **CVE ID: CVE-2024-42079**		
Out-of-bounds Write	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address access struct rdma_restrack_entry's kern_name was set to KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this	https://git.kernel.org/stable/c/782bdaf9d01658281bc813f3f873e6258aa1fd8d, https://git.kernel.org/stable/c/8656ef8a9288d6c932654f8d3856dc4ab1cfc6b5, https://git.kernel.org/stable/c/8ac281d42337f36cf7061cf1ea094181b84bc1a9	O-LIN-LINU-020824/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdma_restrack_entry, it would cause a invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one forgotten PD release in one of the ULPs. But it is not needed anymore, so delete them. **CVE ID: CVE-2024-42080**		
Allocation of Resources Without Limits or Throttling	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It	https://git.kernel.org/stable/c/1095b8efbb13a6a5fa583ed373ee1ccab29da2d0, https://git.kernel.org/stable/c/14e51ea78b4ccacb7acb1346b9241bb790a2054c, https://git.kernel.org/stable/c/1d3e3b3aa2cbe9bc7db9a7f8673a9fa6d2990d54	O-LIN-LINU-020824/499

CVSS 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
			returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation. Thus, there is no sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_live+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b		

CVSS 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
			0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Found by Linux Verification Center (linuxtesting.org) with syzkaller. **CVE ID: CVE-2024-42082**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.9.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	30-Jul-2024	7.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero Avoid potentially reusing uninitialized data **CVE ID: CVE-2024-42225**	https://git.kernel.org/stable/c/22ea2a7f0b64d323625950414a4496520fb33657, https://git.kernel.org/stable/c/64f86337ccfe77fe3be5a9356b0dabde23fbb074, https://git.kernel.org/stable/c/7f819a2f4fbc510e088b49c79addcf1734503578	O-LIN-LINU-020824/500
Use of Uninitialized Resource	30-Jul-2024	7	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Using uninitialized value *size when calling amdgpu_vce_cs_reloc Initialize the size before calling amdgpu_vce_cs_reloc, such as case 0x03000001. V2: To really improve the handling we would actually need to have a separate value of 0xffffffff.(Christian)	https://git.kernel.org/stable/c/855ae72c20310e5402b2317fc537d911e87537ef, https://git.kernel.org/stable/c/88a9a467c548d0b3c7761b4fd54a68e70f9c0944, https://git.kernel.org/stable/c/f8f120b3de48b8b6bdf8988a9b334c2d61c17440	O-LIN-LINU-020824/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42228		
Incorrect Calculation	30-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix calc_available_free_space() for zoned mode calc_available_free_space() returns the total size of metadata (or system) block groups, which can be allocated from unallocated disk space. The logic is wrong on zoned mode in two places. First, the calculation of data_chunk_size is wrong. We always allocate one zone as one chunk, and no partial allocation of a zone. So, we should use zone_size (= data_sinfo->chunk_size) as it is.	https://git.kernel.org/stable/c/64d2c847ba380e07b9072d65a50aa6469d2aa43f, https://git.kernel.org/stable/c/8548903b1999bba02a2b894ad750ab8eb1f40307	O-LIN-LINU-020824/502

CVSS 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
			Second, the result "avail" may not be zone aligned. Since we always allocate one zone as one chunk on zoned mode, returning non-zone size aligned bytes will result in less pressure on the async metadata reclaim process. This is serious for the nearly full state with a large zone size device. Allowing over-commit too much will result in less async reclaim work and end up in ENOSPC. We can align down to the zone size to avoid that. **CVE ID: CVE-2024-42231**		
N/A	30-Jul-2024	4.4	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with kexec	https://git.kernel.org/stable/c/21a741eb75f80397e5f7d3739e24d7d75e619011, https://git.kernel.org/stable/c/8c6506616386ce37e59b2745fc481c6713fae4f3	O-LIN-LINU-020824/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kexec on pseries disables AIL (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can execute scv instructions after AIL is disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to disable AIL after other CPUs have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head code probably couldn't easily deal with implementing such high addresses so it was just decided not to support that interrupt at all.	, https://git.kernel.org/stable/c/c550679d604798d9fed8a5b2bb5693448a25407c	

CVSS 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-2024-42230		
N/A	30-Jul-2024	4.1	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accomplish this by using kfree_sensitive for buffers that previously held the private key. **CVE ID: CVE-2024-42229**	https://git.kernel.org/stable/c/23e4099bdc3c8381992f9eb975c7919 6d6755210, https://git.kernel.org/stable/c/28c8d274848feba552e95c5c2a7e3cfe8f15c534, https://git.kernel.org/stable/c/71dd428615375e36523f4d4f7685ddd54113646d	O-LIN-LINU-020824/504
Affected Version(s): From (including) 6.9 Up to (excluding) 6.9.8					
Improper Initialization	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: initialise nfsd_info.mutex early.	https://git.kernel.org/stable/c/7e8b94045bc77ce4f085ddfb9eb04e5760e66169, https://git.kernel.org/stable/c/e0011bca603c1	O-LIN-LINU-020824/505

CVSS 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
			nfsd_info.mutex can be dereferenced by svc_pool_stats_start() immediately after the new netns is created. Currently this can trigger an oops. Move the initialisation earlier before it can possibly be dereferenced. **CVE ID: CVE-2024-42078**	01f2a3c007bdb77f7006fa78fb1	
Affected Version(s): From (including) 6.9.1 Up to (excluding) 6.9.8					
N/A	29-Jul-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix may_goto with negative offset. Zac's syzbot crafted a bpf prog that exposed two bugs in may_goto. The 1st bug is the way may_goto is patched. When offset is negative it should be patched differently.	https://git.kernel.org/stable/c/175827e04f4be53f3dfb57edf12d0d49b18fd939, https://git.kernel.org/stable/c/2b2efe1937ca9f8815884bd4dcd5b32733025103	O-LIN-LINU-020824/506

CVSS 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 2nd bug is in the verifier: when current state may_goto_depth is equal to visited state may_goto_depth it means there is an actual infinite loop. It's not correct to prune exploration of the program at this point. Note, that this check doesn't limit the program to only one may_goto insn, since 2nd and any further may_goto will increment may_goto_depth only in the queued state pushed for future exploration. The current state will have may_goto_depth == 0 regardless of number of may_goto insns and the verifier has to explore the program until bpf_exit. **CVE ID: CVE-2024-42072**		
Excessive Iteration	29-Jul-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/84b767f9e34fd	O-LIN-LINU-020824/507

CVSS 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: ionic: use dev_consume_skb_ any outside of napi If we're not in a NAPI softirq context, we need to be careful about how we call napi_consume_skb( ), specifically we need to call it with budget==0 to signal to it that we're not in a safe context. This was found while running some configuration stress testing of traffic and a change queue config loop running, and this curious note popped out: [4371.402645] BUG: using smp_processor_id() in preemptible [00000000] code: ethtool/20545	b143c09e66a2a20722fc2921821, https://git.kernel.org/stable/c/ef7646ed49fff962e97b276f4ab91327a67eeb5a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[4371.402897] caller is napi_skb_cache_put +0x16/0x80 [4371.403120] CPU: 25 PID: 20545 Comm: ethtool Kdump: loaded Tainted: G OE 6.10.0-rc3-netnext+ #8 [4371.403302] Hardware name: HPE ProLiant DL360 Gen10/ProLiant DL360 Gen10, BIOS U32 01/23/2021 [4371.403460] Call Trace: [4371.403613] <TASK> [4371.403758] dump_stack_lvl+0x4f/0x70 [4371.403904] check_preemption_disabled+0xc1/0xe0 [4371.404051] napi_skb_cache_put +0x16/0x80 [4371.404199] ionic_tx_clean+0x18a/0x240 [ionic] [4371.404354] ionic_tx_cq_service +0xc4/0x200 [ionic]		

CVSS 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
			[4371.404505] ionic_tx_flush+0x15/0x70 [ionic] [4371.404653] ? ionic_lif_qcq_deinit.isra.23+0x5b/0x70 [ionic] [4371.404805] ionic_txrx_deinit+0x71/0x190 [ionic] [4371.404956] ionic_reconfigure_queues+0x5f5/0xff0 [ionic] [4371.405111] ionic_set_ringparam+0x2e8/0x3e0 [ionic] [4371.405265] ethnl_set_rings+0x1f1/0x300 [4371.405418] ethnl_default_set_doit+0xbb/0x160 [4371.405571] genl_family_rcv_msg_doit+0xff/0x130 [...] I found that ionic_tx_clean() calls napi_consume_skb() which calls napi_skb_cache_put(), but before that last call is the note /* Zero budget indicate non-NAPI		

CVSS 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
			context called us, like netpoll */ and DEBUG_NET_WARN_ON_ONCE(!in_softirq()); Those are pretty big hints that we're doing it wrong. We can pass a context hint down through the calls to let ionic_tx_clean() know what we're doing so it can call napi_consume_skb() correctly. **CVE ID: CVE-2024-42071**		
Use After Free	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix remap of arena. The bpf arena logic didn't account for mremap operation. Add a refcnt for multiple mmap events to prevent use-after-free in arena_vm_close.	https://git.kernel.org/stable/c/87496a1b01e8e2e399428c0db25e106f7961d01e, https://git.kernel.org/stable/c/b90d77e5fd784ada62ddd714d15ee2400c28e1cf	O-LIN-LINU-020824/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42075		
NULL Pointer Dereference	29-Jul-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ionic: fix kernel panic due to multi-buffer handling Currently, the ionic_run_xdp() doesn't handle multi-buffer packets properly for XDP_TX and XDP_REDIRECT. When a jumbo frame is received, the ionic_run_xdp() first makes xdp frame with all necessary pages in the rx descriptor. And if the action is either XDP_TX or XDP_REDIRECT, it should unmap dma-mapping and reset page pointer to NULL for all pages, not only the first page. But it doesn't for SG pages. So, SG pages unexpectedly will be reused.	https://git.kernel.org/stable/c/8ae401525ae84228a8986bb369224a6224e4d22f, https://git.kernel.org/stable/c/e3f02f32a05009a688a87f5799e049ed6b55bab5	O-LIN-LINU-020824/509

CVSS 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 eventually causes kernel panic. Oops: general protection fault, probably for non-canonical address 0x504f4e4dbebc64 ff: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 0 Comm: swapper/3 Not tainted 6.10.0-rc3+ #25 RIP: 0010:xdp_return_frame+0x42/0x90 Code: 01 75 12 5b 4c 89 e6 5d 31 c9 41 5c 31 d2 41 5d e9 73 fd ff ff 44 8b 6b 20 0f b7 43 0a 49 81 ed 68 01 00 00 49 29 c5 49 01 fd <41> 80 7d0 RSP: 0018:ffff99d00122ce08 EFLAGS: 00010202 RAX: 0000000000005453 RBX: ffff8d325f904000 RCX: 0000000000000001 RDX: 00000000670e1000 RSI: 000000011f90d00		

CVSS 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
			0 RDI: 504f4e4d4c4b4a49 RBP: ffff99d003907740 R08: 0000000000000000 R09: 0000000000000000 R10: 000000011f90d000 R11: 0000000000000000 R12: ffff8d325f904010 R13: 504f4e4dbebc64fd R14: ffff8d3242b070c8 R15: ffff99d0039077c0 FS: 0000000000000000(0000) GS:ffff8d399f780000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f41f6c85e38 CR3: 000000037ac30000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace:		

CVSS 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
			<IRQ> ? die_addr+0x33/0x90 ? exc_general_protection+0x251/0x2f0 ? asm_exc_general_protection+0x22/0x30 ? xdp_return_frame+0x42/0x90 ionic_tx_clean+0x211/0x280 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_tx_cq_service+0xd3/0x210 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_txrx_napi+0x41/0x1b0 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] __napi_poll.constprop.0+0x29/0x1b0 net_rx_action+0x2c4/0x350		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle_softirqs+0xf4/0x320 irq_exit_rcu+0x78/0xa0 common_interrupt+0x77/0x90 **CVE ID: CVE-2024-42083**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
N/A	22-Jul-2024	9.8	ProtonVPN before 3.2.10 on Windows mishandles the drive installer path, which should use this: "" + ExpandConstant('{autopf}\Proton\Drive') + "" in Setup/setup.iss. **CVE ID: CVE-2024-37391**	https://github.com/ProtonVPN/win-app/commit/2e4e25036842aaf48838c6a59f14671b86c20aa7, https://github.com/ProtonVPN/win-app/compare/3.2.9...3.2.10	O-MIC-WIND-020824/510
Vendor: Tenda					
Product: o3_firmware1.0.0.10\(2478\)					
Affected Version(s): *					
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability classified as critical was found in Tenda O3 1.0.0.10. This vulnerability affects the function formQosSet. The manipulation of the argument remark/ipRange/upSpeed/downSpee	N/A	O-TEN-O3_F-020824/511

CVSS 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
			d/enable leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272116. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6962**		
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability, which was classified as critical, has been found in Tenda O3 1.0.0.10. This issue affects the function formexeCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272117 was assigned to this vulnerability.	N/A	O-TEN-O3_F-020824/512

CVSS 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
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6963**		
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability, which was classified as critical, was found in Tenda O3 1.0.0.10. Affected is the function fromDhcpSetSer. The manipulation of the argument dhcpEn/startIP/endIP/preDNS/altDNS/mask/gateway leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272118 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6964**	N/A	O-TEN-O3_F-020824/513

CVSS 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
Out-of-bounds Write	22-Jul-2024	8.8	A vulnerability has been found in Tenda O3 1.0.0.10 and classified as critical. Affected by this vulnerability is the function fromVirtualSet. The manipulation of the argument ip/localPort/publicPort/app leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272119. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-6965**	N/A	O-TEN-O3_F-020824/514
Vendor: Tendacn					
Product: ac18_firmware					
Affected Version(s): 15.03.3.10					
Out-of-bounds Write	16-Jul-2024	9.8	Tenda AC18 V15.03.3.10_EN was discovered to contain a stack-based buffer overflow vulnerability via	N/A	O-TEN-AC18-020824/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the deviceId parameter at ip/goform/saveParentControlInfo. **CVE ID: CVE-2024-33180**		
Out-of-bounds Write	16-Jul-2024	9.8	Tenda AC18 V15.03.3.10_EN was discovered to contain a stack-based buffer overflow vulnerability via the deviceId parameter at ip/goform/addWifiMacFilter. **CVE ID: CVE-2024-33182**	N/A	O-TEN-AC18-020824/516
Product: fh1201_firmware					
Affected Version(s): 1.2.0.14					
Out-of-bounds Write	24-Jul-2024	9.8	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the PPPOEPassword parameter at ip/goform/QuickIndex. **CVE ID: CVE-2024-41459**	N/A	O-TEN-FH12-020824/517
Out-of-bounds Write	24-Jul-2024	9.8	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow	N/A	O-TEN-FH12-020824/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability via the entrys parameter at ip/goform/RouteStatic. **CVE ID: CVE-2024-41460**		
Out-of-bounds Write	24-Jul-2024	9.8	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the list1 parameter at ip/goform/DhcpListClient. **CVE ID: CVE-2024-41461**	N/A	O-TEN-FH12-020824/519
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the page parameter at ip/goform/DhcpListClient. **CVE ID: CVE-2024-41462**	N/A	O-TEN-FH12-020824/520
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the entrys parameter at	N/A	O-TEN-FH12-020824/521

CVSS 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/goform/addressNat. **CVE ID: CVE-2024-41463**		
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the mitInterface parameter in ip/goform/RouteStatic **CVE ID: CVE-2024-41464**	N/A	O-TEN-FH12-020824/522
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the funcpara1 parameter at ip/goform/setcfm. **CVE ID: CVE-2024-41465**	N/A	O-TEN-FH12-020824/523
Out-of-bounds Write	24-Jul-2024	7.5	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the page parameter at ip/goform/NatStaticSetting.	N/A	O-TEN-FH12-020824/524

CVSS 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-2024-41466		
Product: i29_firmware					
Affected Version(s): 1.0.0.5					
Use of Hard-coded Credentials	16-Jul-2024	9.8	Tenda i29V1.0 V1.0.0.5 was discovered to contain a hardcoded password for root. **CVE ID: CVE-2024-35338**	N/A	O-TEN-I29_-020824/525
Vendor: totolink					
Product: a6000r_firmware					
Affected Version(s): 1.0.1-b20201211.2000					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Jul-2024	9.8	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the cmd parameter in the webcmd function. **CVE ID: CVE-2024-41319**	N/A	O-TOT-A600-020824/526

CVSS 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