National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 – 31 Aug 2024 Vol. 11 No. 16

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: 7-twenty					
Product: bot					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	5.4	7Twenty - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID: CVE-2024-42335**	N/A	A-7-T-BOT-030924/1
Vendor: Adobe					
Product: experience_manager					
Affected Version(s): * Up to (excluding) 2024.03					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41877**	https://helpx.adobe.com/security/products/experience-manager/apsb24-05.html	A-ADO-EXPE-030924/2

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. **CVE ID: CVE-2024-41878**	https://helpx.adobe.com/security/products/experience-manager/apsb24-05.html	A-ADO-EXPE-030924/3
Affected Version(s): * Up to (excluding) 2024.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/4

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41841		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41843**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/5
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. **CVE ID: CVE-2024-41844**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41845**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/7
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/8

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID: CVE-2024-41846**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-41847**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/9
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the victim's browser. **CVE ID: CVE-2024-41848**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41875**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/11
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the victim's browser. **CVE ID: CVE-2024-41876**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	4.8	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41842**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/13
N/A	23-Aug-2024	4.1	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could lead to a security feature bypass. An low-privileged attacker could leverage this vulnerability to slightly affect the integrity of the page. Exploitation of this issue	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/14

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requires user interaction and scope is changed. **CVE ID: CVE-2024-41849**		
Affected Version(s): * Up to (excluding) 6.5.20.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41877**	https://helpx.adobe.com/security/products/experience-manager/apsb24-05.html	A-ADO-EXPE-030924/15
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to inject and execute arbitrary JavaScript code within the context of the user's browser	https://helpx.adobe.com/security/products/experience-manager/apsb24-05.html	A-ADO-EXPE-030924/16

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. **CVE ID: CVE-2024-41878**		
Affected Version(s): * Up to (excluding) 6.5.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-41841**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/17
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields.	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41843**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41844**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/19
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41845**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41846**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/21
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-41847**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-41848**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/23
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41875**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID: CVE-2024-41876**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/25
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	4.8	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/26

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID: CVE-2024-41842**		
N/A	23-Aug-2024	4.1	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could lead to a security feature bypass. An low-privileged attacker could leverage this vulnerability to slightly affect the integrity of the page. Exploitation of this issue requires user interaction and scope is changed. **CVE ID: CVE-2024-41849**	https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html	A-ADO-EXPE-030924/27
Vendor: adonesevangelista					
Product: laravel_property_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	20-Aug-2024	8.8	A vulnerability was found in itsourcecode Laravel Property Management System 1.0. It has been classified as critical. Affected is the function	N/A	A-ADO-LARA-030924/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UpdateDocuments Request of the file DocumentsController.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7944**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	5.4	A vulnerability was found in itsourcecode Laravel Property Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/notes/create of the component Notes Page. The manipulation of the argument Note text leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-ADO-LARA-030924/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7945		
Product: online_accreditation_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	itsourcecode Online Accreditation Management System contains a Cross Site Scripting vulnerability, which allows an attacker to execute arbitrary code via a crafted payload to the SCHOOLNAME, EMAILADDRES, CONTACTNO, COMPANYNAME and COMPANYCONTACTNO parameters in controller.php. **CVE ID: CVE-2024-42918**	N/A	A-ADO-ONLI-030924/30
Product: online_blood_bank_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file register.php of the component User Signup. The manipulation of the	N/A	A-ADO-ONLI-030924/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument user leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7946**		
Vendor: advancedformintegration					
Product: advanced_form_integration					
Affected Version(s): * Up to (excluding) 1.89.6					
Cross-Site Request Forgery (CSRF)	26-Aug-2024	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Nasirahmed Advanced Form Integration.This issue affects Advanced Form Integration: from n/a through 1.89.4. **CVE ID: CVE-2024-43340**	N/A	A-ADV-ADVA-030924/32
Vendor: Aertherwide					
Product: exiftags					
Affected Version(s): * Up to (including) 1.01					
Out-of-bounds Write	27-Aug-2024	7.8	Buffer Overflow vulnerability in open source exiftags v.1.01 allows a local attacker to execute arbitrary code via the paresetag function. **CVE ID: CVE-2024-42851**	N/A	A-AER-EXIF-030924/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: angeljudesuarez					
Product: billing_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Aug-2024	9.8	A vulnerability was found in itsourcecode Billing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /addclient1.php. The manipulation of the argument lname/fname/mi/address/contact/meterReader leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7913**	N/A	A-ANG-BILL-030924/34
Product: tailoring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Aug-2024	9.8	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. This vulnerability affects unknown code of the file staffcatedit.php. The manipulation	N/A	A-ANG-TAIL-030924/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument title leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8171**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file staffedit.php. The manipulation of the argument id/stafftype/address/fullname/phonenumber/salary leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8220**	N/A	A-ANG-TAIL-030924/36
Vendor: Apache					
Product: airflow					
Affected Version(s): * Up to (excluding) 2.10.0					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-2024	6.1	Apache Airflow, versions before 2.10.0, have a vulnerability that allows the developer of a malicious provider to execute a cross-site scripting attack when clicking on a provider documentation link. This would require the provider to be installed on the web server and the user to click the provider link. Users should upgrade to 2.10.0 or later, which fixes this vulnerability. **CVE ID: CVE-2024-41937**	https://github.com/apache/airflow/pull/40933	A-APA-AIRF-030924/37
Product: hertzbeat					
Affected Version(s): * Up to (excluding) 1.6.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	Hertzbeat is an open source, real-time monitoring system. Hertzbeat 1.6.0 and earlier declares a /api/monitor/{monitorId}/metric/{metricFull} endpoint to download job metrics. In the process, it executes a SQL query with user-controlled	https://github.com/dromara/hertzbeat/blob/1f12ac9f2a1a3d86b1d476775e14174243b250a8/manager/src/main/java/org/dromara/hertzbeat/manager/controller/MonitorsController.java#L202	A-APA-HERT-030924/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data, allowing for SQL injection. **CVE ID: CVE-2024-42361**		
Deserialization of Untrusted Data	20-Aug-2024	8.8	Hertzbeat is an open source, real-time monitoring system. Hertzbeat has an authenticated (user role) RCE via unsafe deserialization in /api/monitors/import. This vulnerability is fixed in 1.6.0. **CVE ID: CVE-2024-42362**	https://github.com/apache/hertzbeat/commit/79f5408e345e8e89da97be05f43e3204a950ddfb, https://github.com/apache/hertzbeat/commit/9dbbfb7812fc4440ba72bdee66799edd519d06bb, https://github.com/apache/hertzbeat/pull/1611	A-APA-HERT-030924/39
Product: portable_runtime					
Affected Version(s): From (including) 0.9.0 Up to (excluding) 1.7.5					
Incorrect Permission Assignment for Critical Resource	26-Aug-2024	5.5	Lax permissions set by the Apache Portable Runtime library on Unix platforms would allow local users read access to named shared memory segments, potentially revealing sensitive application data. This issue does not affect non-Unix platforms, or builds with APR_USE_SH	N/A	A-APA-PORT-030924/40

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MEM_SHMGET=1 (apr.h) Users are recommended to upgrade to APR version 1.7.5, which fixes this issue. **CVE ID: CVE-2023-49582**		
Product: seatunnel					
Affected Version(s): 1.0.0					
Files or Directories Accessible to External Parties	21-Aug-2024	7.5	Mysql security vulnerability in Apache SeaTunnel. Attackers can read files on the MySQL server by modifying the information in the MySQL URL allowLoadLocalInfile=true&allowUrlInLocalInfile=true&allowLoadLocalInfileInPath=/&maxAllowedPacket=655360 This issue affects Apache SeaTunnel: 1.0.0. Users are recommended to upgrade to version	https://lists.apache.org/thread/48j9f1nsn037mgzc4j9o51nwglb1s08h	A-APA-SEAT-030924/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[1.0.1], which fixes the issue. **CVE ID: CVE-2023-49198**		
Vendor: apolloconfig					
Product: apollo					
Affected Version(s): * Up to (excluding) 2.3.0					
N/A	20-Aug-2024	4.3	Apollo is a configuration management system. A vulnerability exists in the synchronization configuration feature that allows users to craft specific requests to bypass permission checks. This exploit enables them to modify a namespace without the necessary permissions. The issue was addressed with an input parameter check which was released in version 2.3.0. **CVE ID: CVE-2024-43397**	https://github.com/apolloconfig/apollo/commit/f55b419145bf9d4f2f51dd4cd45108229e8d97ed, https://github.com/apolloconfig/apollo/pull/5192, https://github.com/apolloconfig/apollo/security/advisories/GHSA-c6c3-h4f7-3962	A-APO-APOL-030924/42
Affected Version(s): 2.2.0					
N/A	20-Aug-2024	7.5	An issue in apollocongif apollo v.2.2.0 allows a remote attacker to obtain sensitive information via a crafted request.	N/A	A-APO-APOL-030924/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42662		
Vendor: appcheap					
Product: app_builder					
Affected Version(s): * Up to (excluding) 4.3.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Aug-2024	7.5	The App Builder – Create Native Android & iOS Apps On The Flight plugin for WordPress is vulnerable to limited SQL Injection via the 'app-builder-search' parameter in all versions up to, and including, 4.2.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-7651**	https://plugins.trac.wordpress.org/browser/app-builder/trunk/includes/pure.php#L18	A-APP-APP_-030924/44
Vendor: arajajyothibabu					
Product: school_management_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2020-06-20					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the password parameter at login.php **CVE ID: CVE-2024-42566**	N/A	A-ARA-SCHO-030924/45
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the sid parameter at /search.php?action=2. **CVE ID: CVE-2024-42567**	N/A	A-ARA-SCHO-030924/46
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the transport parameter at vehicle.php. **CVE ID: CVE-2024-42568**	N/A	A-ARA-SCHO-030924/47

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at admininsert.php. **CVE ID: CVE-2024-42570**	N/A	A-ARA-SCHO-030924/48
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at unitmarks.php. **CVE ID: CVE-2024-42572**	N/A	A-ARA-SCHO-030924/49
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at dtmarks.php. **CVE ID: CVE-2024-42573**	N/A	A-ARA-SCHO-030924/50
Improper Neutralization of	20-Aug-2024	9.8	School Management System commit	N/A	A-ARA-SCHO-030924/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at attendance.php. **CVE ID: CVE-2024-42574**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at substaff.php. **CVE ID: CVE-2024-42575**	N/A	A-ARA-SCHO-030924/52
Vendor: Autodesk					
Product: revit					
Affected Version(s): 2022					
Out-of-bounds Write	21-Aug-2024	7.8	A maliciously crafted DWG file, when parsed in Revit, can force a stack-based buffer overflow. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID: CVE-2024-37008**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0013	A-AUT-REVI-030924/53

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2023					
Out-of-bounds Write	21-Aug-2024	7.8	A maliciously crafted DWG file, when parsed in Revit, can force a stack-based buffer overflow. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID: CVE-2024-37008**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0013	A-AUT-REVI-030924/54
Affected Version(s): 2024					
Out-of-bounds Write	21-Aug-2024	7.8	A maliciously crafted DWG file, when parsed in Revit, can force a stack-based buffer overflow. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID: CVE-2024-37008**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0013	A-AUT-REVI-030924/55
Affected Version(s): 2025					
Out-of-bounds Write	21-Aug-2024	7.8	A maliciously crafted DWG file, when parsed in Revit, can force a stack-based buffer overflow. A malicious actor can leverage this vulnerability to	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0013	A-AUT-REVI-030924/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code in the context of the current process. **CVE ID: CVE-2024-37008**		
Vendor: bitapps					
Product: contact_form_builder					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.13.10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Aug-2024	9	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable to arbitrary file read and deletion due to insufficient file path validation in multiple functions in versions 2.0 to 2.13.9. This makes it possible for authenticated attackers, with Administrator-level access and above, to read and delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	https://plugins.trac.wordpress.org/browser/bit-form/tags/2.13.3/includes/Admin/AdminAjax.php#L829, https://plugins.trac.wordpress.org/browser/bit-form/tags/2.13.3/includes/Admin/AdminAjax.php#L852	A-BIT-CONT-030924/57

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7777		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	7.2	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable to generic SQL Injection via the entryID parameter in versions 2.0 to 2.13.9 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 Administrator-level access and above, to append additional SQL queries to already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-7702**	https://plugins.trac.wordpress.org/browser/bit-form/trunk/includes/Admin/AdminAjax.php#L944	A-BIT-CONT-030924/58
Improper Neutralizat	20-Aug-2024	7.2	The Contact Form by Bit Form: Multi	https://plugins.trac.wordpress.	A-BIT-CONT-030924/59

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable to generic SQL Injection via the id parameter in versions 2.0 to 2.13.9 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 Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-7780**	org/browser/bit-form/tags/2.13.6/includes/Admin/AdminAjax.php#L1108, https://plugins.trac.wordpress.org/browser/bit-form/tags/2.13.6/includes/Admin/Form/AdminFormHandler.php#L2387	
Improper Neutralization of Input During Web Page	20-Aug-2024	4.8	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment	https://plugins.trac.wordpress.org/browser/bit-form/tags/2.13.	A-BIT-CONT-030924/60

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable to arbitrary JavaScript file uploads due to missing input validation in the addCustomCode function in versions 2.0 to 2.13.9. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary JavaScript files to the affected site's server. **CVE ID: CVE-2024-7775**	6/includes/Admin/AdminAjax.php#L1314	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.13.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Aug-2024	6.5	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the iconRemove function in versions 2.0 to 2.13.4. This	https://plugins.trac.wordpress.org/browser/bit-form/tags/2.13.0/includes/Admin/AdminAjax.php#L1271	A-BIT-CONT-030924/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). **CVE ID: CVE-2024-7782**		
Vendor: blood_bank_system_project					
Product: blood_bank_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-2024	6.1	A vulnerability has been found in code-projects Blood Bank System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /login.php of the component Login Page. The manipulation of the argument user leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-BLO-BLOO-030924/62

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8174		
Vendor: bobbingwide					
Product: oik					
Affected Version(s): * Up to (excluding) 4.12.1					
Cross-Site Request Forgery (CSRF)	26-Aug-2024	4.3	Cross-Site Request Forgery (CSRF) vulnerability in bobbingwide.This issue affects oik: from n/a through 4.12.0. **CVE ID: CVE-2024-43356**	N/A	A-BOB-OIK-030924/63
Vendor: brainlowcode					
Product: brain_low-code					
Affected Version(s): * Up to (excluding) 2.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 564 - SQL Injection: Hibernate vulnerability in Brain Information Technologies Inc. Brain Low-Code allows SQL Injection.This issue affects Brain Low-Code: before 2.1.0. **CVE ID: CVE-2024-7071**	N/A	A-BRA-BRAI-030924/64
Vendor: casbin					
Product: casdoor					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Comparison	20-Aug-2024	8.8	Casdoor is a UI-first Identity and Access Management (IAM) / Single-Sign-On (SSO) platform. In Casdoor 1.577.0 and earlier, a logic vulnerability exists in the beego filter CorsFilter that allows any website to make cross domain requests to Casdoor as the logged in user. Due to the a logic error in checking only for a prefix when authenticating the Origin header, any domain can create a valid subdomain with a valid subdomain prefix (Ex: localhost.example.com), allowing the website to make requests to Casdoor as the current signed-in user. **CVE ID: CVE-2024-41657**	N/A	A-CAS-CASD-030924/65
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	6.1	Casdoor is a UI-first Identity and Access Management (IAM) / Single-Sign-On (SSO) platform. In Casdoor 1.577.0 and earlier, he purchase URL that is created to	N/A	A-CAS-CASD-030924/66

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generate a WechatPay QR code is vulnerable to reflected XSS. When purchasing an item through casdoor, the product page allows you to pay via wechat pay. When using wechat pay, a QR code with the wechat pay link is displayed on the payment page, hosted on the domain of casdoor. This page takes a query parameter from the url successUrl, and redirects the user to that url after a successful purchase. Because the user has no reason to think that the payment page contains sensitive information, they may share it with other or can be social engineered into sending it to others. An attacker can then craft the casdoor link with a special url and send it back to the user, and once payment has gone though an XSS attack occurs.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41658		
Vendor: chartist					
Product: chartist					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.3.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	29-Aug-2024	9.8	Chartist 1.x through 1.3.0 allows Prototype Pollution via the extend function. **CVE ID: CVE-2024-45435**	N/A	A-CHA-CHAR-030924/67
Vendor: Ckeditor					
Product: ckeditor					
Affected Version(s): From (including) 4.0 Up to (excluding) 4.25.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-2024	6.1	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A potential vulnerability has been discovered in CKEditor 4 Code Snippet GeSHi plugin. The vulnerability allowed a reflected XSS attack by exploiting a flaw in the GeSHi syntax highlighter library hosted by the victim. The GeSHi library was included as a vendor dependency in CKEditor 4 source files. In a specific scenario, an	https://github.com/ckeditor/ckeditor4/commit/71072c9f7f263329841bd38e7e5309074c82ef94, https://github.com/ckeditor/ckeditor4/commit/951e7d75fcbcaa2590b0719fb0bb0dd0539ca6fa, https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-7r32-vfj5-c2jv	A-CKE-CKED-030924/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could craft a malicious script that could be executed by sending a request to the GeSHi library hosted on a PHP web server. The GeSHi library is no longer actively maintained. Due to the lack of ongoing support and updates, potential security vulnerabilities have been identified with its continued use. To mitigate these risks and enhance the overall security of the CKEditor 4, we have decided to completely remove the GeSHi library as a dependency. This change aims to maintain a secure environment and reduce the risk of any security incidents related to outdated or unsupported software. The fix is be available in version 4.25.0-lts. **CVE ID: CVE-2024-43407**		
Vendor: corydolphin					
Product: flask-cors					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.0.1					
N/A	18-Aug-2024	7.5	A vulnerability in corydolphin/flask-cors version 4.0.1 allows the `Access-Control-Allow-Private-Network` CORS header to be set to true by default, without any configuration option. This behavior can expose private network resources to unauthorized external access, leading to significant security risks such as data breaches, unauthorized access to sensitive information, and potential network intrusions. **CVE ID: CVE-2024-6221**	N/A	A-COR-FLAS-030924/69
Vendor: cridio					
Product: listingpro					
Affected Version(s): * Up to (including) 2.9.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro allows SQL Injection.This issue affects	N/A	A-CRI-LIST-030924/70

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ListingPro: from n/a through 2.9.4. **CVE ID: CVE-2024-38795**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro.This issue affects ListingPro: from n/a through 2.9.4. **CVE ID: CVE-2024-39622**	N/A	A-CRI-LIST-030924/71
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro allows SQL Injection.This issue affects ListingPro: from n/a through 2.9.4. **CVE ID: CVE-2024-39620**	N/A	A-CRI-LIST-030924/72
Vendor: cryoutcreations					
Product: esotera					
Affected Version(s): * Up to (including) 1.2.5.1					
Improper Neutralization of Input During Web Page	29-Aug-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site	N/A	A-CRY-ESOT-030924/73

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting') vulnerability in CryoutCreations Esotera allows Stored XSS.This issue affects Esotera: from n/a through 1.2.5.1. **CVE ID: CVE-2024-43952**		
Product: tempera					
Affected Version(s): * Up to (including) 1.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Aug-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Tempera allows Stored XSS.This issue affects Tempera: from n/a through 1.8.2. **CVE ID: CVE-2024-43951**	N/A	A-CRY-TEMP-030924/74
Vendor: cyberark					
Product: identity					
Affected Version(s): *					
Exposure of Sensitive Information to an Unauthorized Actor	25-Aug-2024	6.5	CyberArk - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor **CVE ID: CVE-2024-42337**	N/A	A-CYB-IDEN-030924/75
Exposure of Sensitive Informatio	25-Aug-2024	4.3	CyberArk - CWE-200: Exposure of Sensitive	N/A	A-CYB-IDEN-030924/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to an Unauthorized Actor			Information to an Unauthorized Actor **CVE ID: CVE-2024-42338**		
N/A	25-Aug-2024	4.3	CyberArk - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor **CVE ID: CVE-2024-42339**	N/A	A-CYB-IDEN-030924/77
N/A	25-Aug-2024	4.3	CyberArk - CWE-602: Client-Side Enforcement of Server-Side Security **CVE ID: CVE-2024-42340**	N/A	A-CYB-IDEN-030924/78
Vendor: dedebiz					
Product: dedebiz					
Affected Version(s): 6.3.0					
Unrestricted Upload of File with Dangerous Type	18-Aug-2024	8.8	A vulnerability was found in DedeBIZ 6.3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin/media_add.php of the component File Extension Handler. The manipulation of the argument upfile1 leads to unrestricted upload. The attack can be launched remotely. The	N/A	A-DED-DEDE-030924/79

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7903**		
Unrestricted Upload of File with Dangerous Type	18-Aug-2024	8.8	A vulnerability was found in DedeBIZ 6.3.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/file_manage_control.php of the component File Extension Handler. The manipulation of the argument upfile1 leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-DED-DEDE-030924/80

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7904		
Unrestricted Upload of File with Dangerous Type	18-Aug-2024	7.2	A vulnerability classified as critical has been found in DedeBIZ 6.3.0. This affects the function AdminUpload of the file admin/archives_do.php. The manipulation of the argument litpic leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7905**	N/A	A-DED-DEDE-030924/81
Vendor: Dell					
Product: repository_manager					
Affected Version(s): * Up to (excluding) 3.4.3					
N/A	21-Aug-2024	7.8	Dell Repository Manager version 3.4.2 and earlier, contain a Local Privilege Escalation Vulnerability in Installation module. A local low	https://www.dell.com/support/kbdoc/en-us/000207513/dsa-2023-017-dell-emc-repository-manager-drm-	A-DEL-REPO-030924/82

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker may potentially exploit this vulnerability leading to the execution of arbitrary executable on the operating system with high privileges using the existing vulnerability in operating system. Exploitation may lead to unavailability of the service. **CVE ID: CVE-2023-22576**	security-update-for-an-improper-privilege-management-vulnerability	
Vendor: demozx					
Product: gf_cms					
Affected Version(s): From (including) 1.0 Up to (excluding) 1.0.2					
Use of Hard-coded Credentials	20-Aug-2024	9.8	A vulnerability was found in demozx gf_cms 1.0/1.0.1. It has been classified as critical. This affects the function init of the file internal/logic/auth/auth.go of the component JWT Authentication. The manipulation leads to hard-coded credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be	https://github.com/demozx/gf_cms/commit/be702ada7cb6fdabc02689d90b38139c827458a5, https://github.com/demozx/gf_cms/commit/de51cc57a96ccca905c837ef925c2cc3a5241383	A-DEM-GF_C-030924/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. Upgrading to version 1.0.2 is able to address this issue. The patch is named be702ada7cb6fdabc02689d90b38139c827458a5. It is recommended to upgrade the affected component. **CVE ID: CVE-2024-8005**		
Vendor: donbermoy					
Product: e-commerce_website					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	A vulnerability has been found in SourceCodester E-Commerce Website 1.0 and classified as critical. This vulnerability affects unknown code of the file /Admin/registration.php. The manipulation of the argument fname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8217**	N/A	A-DON-E-CO-030924/84
Vendor: douco					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: douphp					
Affected Version(s): 1.7					
Unrestricted Upload of File with Dangerous Type	18-Aug-2024	7.2	A vulnerability, which was classified as critical, has been found in DouPHP 1.7 Release 20220822. Affected by this issue is some unknown functionality of the file /admin/system.php of the component Favicon Handler. The manipulation of the argument site_favicon leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7917**	N/A	A-DOU-DOUP-030924/85
Vendor: etoilewebdesign					
Product: front_end_users					
Affected Version(s): * Up to (excluding) 3.2.29					
Improper Neutralization of Special Elements used in an SQL Command	29-Aug-2024	8.8	The Front End Users plugin for WordPress is vulnerable to time-based SQL Injection via the 'order' parameter in all versions up to, and including, 3.2.28 due to insufficient	https://plugins.trac.wordpress.org/changeset/3142978/	A-ETO-FRON-030924/86

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-7607**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Aug-2024	5.4	The Front End Users plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'user-search' shortcode in all versions up to, and including, 3.2.28 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level	https://plugins.trac.wordpress.org/changeset/3142978/	A-ETO-FRON-030924/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-7606**		
Vendor: fabianros					
Product: job_portal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Aug-2024	9.8	A vulnerability was found in code-projects Job Portal 1.0. It has been classified as critical. Affected is an unknown function of the file /forget.php. The manipulation of the argument email/mobile leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8167**	N/A	A-FAB-JOB_-030924/88
Product: online_bus_reservation_site					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	26-Aug-2024	9.8	A vulnerability was found in code-projects Online Bus Reservation Site 1.0. It has been	N/A	A-FAB-ONLI-030924/89

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8168**		
Product: online_quiz_site					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Aug-2024	9.8	A vulnerability was found in code-projects Online Quiz Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file signupuser.php. The manipulation of the argument lid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8169**	N/A	A-FAB-ONLI-030924/90

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	A vulnerability was found in code-projects Online Quiz Site 1.0 and classified as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument loginid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8218**	N/A	A-FAB-ONLI-030924/91
Product: responsive_hotel_site					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	A vulnerability was found in code-projects Responsive Hotel Site 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument name/phone/email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	N/A	A-FAB-RESP-030924/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. **CVE ID: CVE-2024-8219**		
Vendor: feehi					
Product: feehicms					
Affected Version(s): * Up to (including) 2.1.1					
Unrestricted Upload of File with Dangerous Type	29-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in FeehiCMS up to 2.1.1. This affects the function update of the file /admin/index.php?r=friendly-link%2Fupdate. The manipulation of the argument FriendlyLink[image] leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8294**	N/A	A-FEE-FEEH-030924/93
Unrestricted Upload of File with	29-Aug-2024	9.8	A vulnerability has been found in FeehiCMS up to	N/A	A-FEE-FEEH-030924/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			2.1.1 and classified as critical. This vulnerability affects the function createBanner of the file /admin/index.php?r=banner%2Fbanner-create. The manipulation of the argument BannerForm[img] leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8295**		
Unrestricted Upload of File with Dangerous Type	29-Aug-2024	9.8	A vulnerability was found in FeehiCMS up to 2.1.1 and classified as critical. This issue affects the function insert of the file /admin/index.php?r=user%2Fcreate. The manipulation of the argument User[avatar] leads to unrestricted upload. The attack	N/A	A-FEE-FEEH-030924/95

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8296**		
Vendor: floraison					
Product: fugit					
Affected Version(s): * Up to (excluding) 1.11.1					
N/A	19-Aug-2024	7.5	fugit contains time tools for flor and the floraison group. The fugit "natural" parser, that turns "every wednesday at 5pm" into "0 17 * * 3", accepted any length of input and went on attempting to parse it, not returning promptly, as expected. The parse call could hold the thread with no end in sight. Fugit dependents that do not check (user) input length for plausibility are impacted. A fix was released in fugit 1.11.1.	https://github.com/floraison/fugit/commit/ad2c1c9c737213d585fff0b51c927d178b2c05a5, https://github.com/floraison/fugit/issues/104, https://github.com/floraison/fugit/security/advisories/GHSA-2m96-52r3-2f3g	A-FLO-FUGI-030924/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43380		
Vendor: flowiseai					
Product: flowise					
Affected Version(s): 1.8.2					
Improper Authentication	27-Aug-2024	8.1	An Authentication Bypass vulnerability exists in Flowise version 1.8.2. This could allow a remote, unauthenticated attacker to access API endpoints as an administrator and allow them to access restricted functionality. **CVE ID: CVE-2024-8181**	N/A	A-FLO-FLOW-030924/97
N/A	27-Aug-2024	7.5	An Unauthenticated Denial of Service (DoS) vulnerability exists in Flowise version 1.8.2 leading to a complete crash of the instance running a vulnerable version due to improper handling of user supplied input to the “/api/v1/get-upload-file” api endpoint. **CVE ID: CVE-2024-8182**	N/A	A-FLO-FLOW-030924/98
Vendor: fortra					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: filecatalyst_workflow					
Affected Version(s): From (including) 5.0.4 Up to (excluding) 5.1.7					
Use of Hard-coded Credentials	27-Aug-2024	9.8	The default credentials for the setup HSQL database (HSQLDB) for FileCatalyst Workflow are published in a vendor knowledgebase article. Misuse of these credentials could lead to a compromise of confidentiality, integrity, or availability of the software. The HSQLDB is only included to facilitate installation, has been deprecated, and is not intended for production use per vendor guides. However, users who have not configured FileCatalyst Workflow to use an alternative database per recommendations are vulnerable to attack from any source that can reach the HSQLDB.	https://www.fortra.com/security/advisories/product-security/fi-2024-011	A-FOR-FILE-030924/99

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-6633		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	7.2	A vulnerability exists in FileCatalyst Workflow whereby a field accessible to the super admin can be used to perform an SQL injection attack which can lead to a loss of confidentiality, integrity, and availability. **CVE ID: CVE-2024-6632**	https://www.fortra.com/security/advisories/product-security/fi-2024-010	A-FOR-FILE-030924/100
Vendor: friendica					
Product: friendica					
Affected Version(s): 2024.03					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	5.4	Friendica 2024.03 is vulnerable to Cross Site Scripting (XSS) in settings/profile via the homepage, xmpp, and matrix parameters. **CVE ID: CVE-2024-39094**	N/A	A-FRI-FRIE-030924/101
Vendor: frrouting					
Product: frrouting					
Affected Version(s): * Up to (including) 10.1					
N/A	19-Aug-2024	7.5	An issue was discovered in FRRouting (FRR) through 10.1. bgp_attr_encap in bgpd/bgp_attr.c	https://github.com/FRRouting/frr/pull/16497	A-FRR-FRRO-030924/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not check the actual remaining stream length before taking the TLV value. **CVE ID: CVE-2024-44070**		
Vendor: getbrave					
Product: brave					
Affected Version(s): * Up to (excluding) 0.7.1					
Cross-Site Request Forgery (CSRF)	26-Aug-2024	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Brave Brave Popup Builder.This issue affects Brave Popup Builder: from n/a through 0.7.0. **CVE ID: CVE-2024-43337**	N/A	A-GET-BRAV-030924/103
Vendor: ghost					
Product: ghost					
Affected Version(s): From (including) 4.46.0 Up to (excluding) 5.89.5					
Improper Authentication	20-Aug-2024	6.5	Ghost is a Node.js content management system. Improper authentication on some endpoints used for member actions would allow an attacker to perform member-only actions, and read member information. This security vulnerability is present in Ghost v4.46.0-v5.89.4.	https://github.com/TryGhost/Ghost/commit/dac25612520b571f58679764ecc27109e641d1db, https://github.com/TryGhost/Ghost/security/advisories/GHSA-78x2-cwp9-5j42	A-GHO-GHOS-030924/104

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v5.89.5 contains a fix for this issue. **CVE ID: CVE-2024-43409**		
Vendor: gianniporto					
Product: intothedark					
Affected Version(s): * Up to (including) 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Aug-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gianni Porto IntoTheDark allows Reflected XSS.This issue affects IntoTheDark: from n/a through 1.0.5. **CVE ID: CVE-2024-43958**	N/A	A-GIA-INTO-030924/105
Vendor: gitapp					
Product: dingfanzu					
Affected Version(s): * Up to (including) 2024-01-31					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	A vulnerability was found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax/checkin.php. The manipulation	N/A	A-GIT-DING-030924/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8301**		
Vendor: givewp					
Product: givewp					
Affected Version(s): * Up to (excluding) 3.14.0					
Missing Authorization	20-Aug-2024	5.3	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'setup_wizard' function in all versions up to, and	https://plugins.trac.wordpress.org/browser/give/tags/3.12.0/src/Onboarding/Wizard/Page.php#L78, https://plugins.trac.wordpress.org/changeset/3120745/	A-GIV-GIVE-030924/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 3.13.0. This makes it possible for unauthenticated attackers to read the setup wizard administrative pages. **CVE ID: CVE-2024-5939**		
Missing Authorization	20-Aug-2024	5.3	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'handle_request' function in all versions up to, and including, 3.13.0. This makes it possible for unauthenticated attackers to edit event ticket settings if the Events beta feature is enabled. **CVE ID: CVE-2024-5940**	https://plugins.trac.wordpress.org/browser/give/tags/3.12.0/src/EventTickets/Routes/UpdateEvent.php#L81, https://plugins.trac.wordpress.org/browser/give/tags/3.12.0/src/EventTickets/Routes/UpdateEventTicketType.php#L78	A-GIV-GIVE-030924/108
Affected Version(s): * Up to (excluding) 3.14.2					
Deserialization of Untrusted Data	20-Aug-2024	9.8	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to PHP	https://plugins.trac.wordpress.org/browser/give/tags/3.12.0/includes/login-register.php#L2	A-GIV-GIVE-030924/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Object Injection in all versions up to, and including, 3.14.1 via deserialization of untrusted input from the 'give_title' parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to execute code remotely, and to delete arbitrary files. **CVE ID: CVE-2024-5932**	35, https://plugins.trac.wordpress.org/browser/give/tags/3.12.0/includes/process-donation.php#L420, https://plugins.trac.wordpress.org/changeset/3132247/	
Missing Authorization	20-Aug-2024	5.4	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to unauthorized access and deletion of data due to a missing capability check on the 'handle_request' function in all versions up to, and including, 3.14.1. This makes it possible for authenticated attackers, with Subscriber-level access and above,	https://plugins.trac.wordpress.org/browser/give/tags/3.12.0/src/DonorDashboards/Tabs/EditProfileTab/AvatarRoute.php#L36, https://plugins.trac.wordpress.org/changeset/3132247/	A-GIV-GIVE-030924/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to read attachment paths and delete attachment files. **CVE ID: CVE-2024-5941**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 128.0.6613.113					
Out-of-bounds Write	28-Aug-2024	8.8	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8193**	N/A	A-GOO-CHRO-030924/111
Access of Resource Using Incompatible Type ('Type Confusion')	28-Aug-2024	8.8	Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8194**	N/A	A-GOO-CHRO-030924/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	28-Aug-2024	8.8	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-8198**	N/A	A-GOO-CHRO-030924/113
Affected Version(s): * Up to (excluding) 128.0.6613.84					
Use After Free	21-Aug-2024	8.8	Use after free in Passwords in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7964**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/114
Out-of-bounds Write	21-Aug-2024	8.8	Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via	N/A	A-GOO-CHRO-030924/115

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7965**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Aug-2024	8.8	Out of bounds memory access in Skia in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had compromised the renderer process to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7966**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/116
Out-of-bounds Write	21-Aug-2024	8.8	Heap buffer overflow in Fonts in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7967**	N/A	A-GOO-CHRO-030924/117
Use After Free	21-Aug-2024	8.8	Use after free in Autofill in Google Chrome prior to	https://chromereleases.googleblog.com/2024	A-GOO-CHRO-030924/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			128.0.6613.84 allowed a remote attacker who had convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7968**	/08/stable-channel-update-for-desktop_21.html	
Access of Resource Using Incompatible Type ('Type Confusion')	21-Aug-2024	8.8	Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7969**	N/A	A-GOO-CHRO-030924/119
Access of Resource Using Incompatible Type ('Type Confusion')	21-Aug-2024	8.8	Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7971**	N/A	A-GOO-CHRO-030924/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Aug-2024	8.8	Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-7972**	N/A	A-GOO-CHRO-030924/121
Out-of-bounds Write	21-Aug-2024	8.8	Heap buffer overflow in PDFium in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file. (Chromium security severity: Medium) **CVE ID: CVE-2024-7973**	N/A	A-GOO-CHRO-030924/122
N/A	21-Aug-2024	8.8	Insufficient data validation in V8 API in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Medium) **CVE ID: CVE-2024-7974**		
N/A	21-Aug-2024	7.8	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium) **CVE ID: CVE-2024-7977**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/124
Insufficient Verification of Data Authenticity	21-Aug-2024	7.8	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium) **CVE ID: CVE-2024-7979**	N/A	A-GOO-CHRO-030924/125
Insufficient Verification of Data Authenticity	21-Aug-2024	7.8	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local	N/A	A-GOO-CHRO-030924/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium) **CVE ID: CVE-2024-7980**		
N/A	21-Aug-2024	4.3	Inappropriate implementation in Permissions in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-7975**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/127
N/A	21-Aug-2024	4.3	Inappropriate implementation in FedCM in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-7976**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/128
N/A	21-Aug-2024	4.3	Insufficient policy enforcement in Data Transfer in Google Chrome	https://chromereleases.googleblog.com/2024/08/stable-	A-GOO-CHRO-030924/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 128.0.6613.84 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID: CVE-2024-7978**	channel-update-for-desktop_21.html	
N/A	21-Aug-2024	4.3	Inappropriate implementation in Views in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID: CVE-2024-7981**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/130
N/A	21-Aug-2024	4.3	Inappropriate implementation in WebApp Installs in Google Chrome on Windows prior to 128.0.6613.84 allowed an attacker who convinced a user to install a malicious application to perform UI spoofing via a crafted HTML page. (Chromium	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/131

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Low) **CVE ID: CVE-2024-8033**		
N/A	21-Aug-2024	4.3	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID: CVE-2024-8034**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/132
N/A	21-Aug-2024	4.3	Inappropriate implementation in Extensions in Google Chrome on Windows prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID: CVE-2024-8035**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	A-GOO-CHRO-030924/133
Vendor: gotribe					
Product: gotribe					
Affected Version(s): * Up to (excluding) 2024-08-23					
Use of Hard-coded Credentials	24-Aug-2024	9.8	A vulnerability classified as critical has been found in Go-Tribe gotribe up	https://github.com/Go-Tribe/gotribe/commit/4fb9b9e	A-GOT-GOTR-030924/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cd3ccd32cd77852c9ea73f986eaf8c301cfb6310. Affected is the function Sign of the file pkg/token/token.go. The manipulation of the argument config.key leads to hard-coded credentials. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as 4fb9b9e80a2beedd09d9fde4b9cf5bd510baf18f. It is recommended to apply a patch to fix this issue. **CVE ID: CVE-2024-8135**	80a2beedd09d9fde4b9cf5bd510baf18f	
Product: gotribe-admin					
Affected Version(s): 1.0					
Deserialization of Untrusted Data	20-Aug-2024	9.8	A vulnerability was found in Go-Tribe gotribe-admin 1.0 and classified as problematic. Affected by this issue is the function InitRoutes of the file	https://github.com/Go-Tribe/gotribe-admin/commit/45ac90d6d1f82716f77dbcdf8e7309c229080e3c	A-GOT-GOTR-030924/135

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal/app/routes/routes.go of the component Log Handler. The manipulation leads to deserialization. The patch is identified as 45ac90d6d1f82716f77dbcdf8e7309c229080e3c. It is recommended to apply a patch to fix this issue. **CVE ID: CVE-2024-8003**		
Vendor: gzequan					
Product: eq_enterprise_management_system					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Aug-2024	9.8	An issue in EQ Enterprise Management System before v2.0.0 allows attackers to execute a directory traversal via crafted requests. **CVE ID: CVE-2024-44761**	N/A	A-GZE-EQ_E-030924/136
Vendor: hargal					
Product: hargal_windows_client					
Affected Version(s): * Up to (excluding) 2401					
Improper Access Control	20-Aug-2024	9.8	Hargal - CWE-284: Improper Access Control **CVE ID: CVE-2024-42334**	N/A	A-HAR-HARG-030924/137
Vendor: Haxx					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: libcurl					
Affected Version(s): -					
N/A	19-Aug-2024	5.9	The libcurl CURLOPT_SSL_VERIFYPEER option was disabled on a subset of requests made by Nest production devices which enabled a potential man-in-the-middle attack on requests to Google cloud services by any host the traffic was routed through. **CVE ID: CVE-2024-32928**	https://support.google.com/product-documentation/answer/14771247?hl=en&ref_topic=12974021&sjid=9111851316942032590-NA#zippy=	A-HAX-LIBC-030924/138
Vendor: Hex-rays					
Product: ida_pro					
Affected Version(s): * Up to (including) 8.4					
Allocation of Resources Without Limits or Throttling	19-Aug-2024	7.5	ida64.dll in Hex-Rays IDA Pro through 8.4 crashes when there is a section that has many jumps linked, and the final jump corresponds to the payload from where the actual entry point will be invoked. NOTE: in many use cases, this is an inconvenience but not a security issue. **CVE ID: CVE-2024-44083**	N/A	A-HEX-IDA_-030924/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: heytap					
Product: internet_browser					
Affected Version(s): 45.10.3.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-2024	6.1	The ColorOS Internet Browser com.heytap.browser application 45.10.3.4.1 for Android allows a remote attacker to execute arbitrary JavaScript code via the com.android.browser.RealBrowserActivity component. **CVE ID: CVE-2024-23729**	https://github.com/actuator/com.heytap.browser	A-HEY-INTE-030924/140
Vendor: hitachienergy					
Product: microscada_x_sys600					
Affected Version(s): * Up to (excluding) 10.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	The product does not validate any query towards persistent data, resulting in a risk of injection attacks. **CVE ID: CVE-2024-4872**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch	A-HIT-MICR-030924/141
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	27-Aug-2024	8.8	The product allows user input to control or influence paths or file names that are used in filesystem operations, allowing the attacker to access	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch	A-HIT-MICR-030924/142

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or modify system files or other files that are critical to the application. **CVE ID: CVE-2024-3980**		
Authentication Bypass by Capture-replay	27-Aug-2024	8.2	An attacker with local access to machine where MicroSCADA X SYS600 is installed, could enable the session logging supporting the product and try to exploit a session hijacking of an already established session. By default, the session logging level is not enabled and only users with administrator rights can enable it. **CVE ID: CVE-2024-3982**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch	A-HIT-MICR-030924/143
URL Redirection to Untrusted Site ('Open Redirect')	27-Aug-2024	6.1	An HTTP parameter may contain a URL value and could cause the web application to redirect the request to the specified URL. By modifying the URL value to a malicious site, an attacker may	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch	A-HIT-MICR-030924/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successfully launch a phishing scam and steal user credentials. **CVE ID: CVE-2024-7941**		
Affected Version(s): From (including) 10.2 Up to (excluding) 10.6					
Missing Authentication for Critical Function	27-Aug-2024	9.8	The product exposes a service that is intended for local only to all network interfaces without any authentication. **CVE ID: CVE-2024-7940**	https://publisher.hitachienergy.com/preview?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch	A-HIT-MICR-030924/145
Vendor: IBM					
Product: app_connect_enterprise_certified_container					
Affected Version(s): 10.0					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/146
Affected Version(s): 10.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/147
Affected Version(s): 11.0					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/148
Affected Version(s): 11.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/149
Affected Version(s): 11.2					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/150
Affected Version(s): 11.3					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/151
Affected Version(s): 11.4					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/152
Affected Version(s): 11.5					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/153
Affected Version(s): 11.6					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/154
Affected Version(s): 12.0					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/155
Affected Version(s): 12.1					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/156
Affected Version(s): 5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/157
Affected Version(s): 7.1					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/158
Affected Version(s): 7.2					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/159
Affected Version(s): 8.0					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/160
Affected Version(s): 8.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/161
Affected Version(s): 8.2					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/162
Affected Version(s): 9.0					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/163
Affected Version(s): 9.1					
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/164
Affected Version(s): 9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	24-Aug-2024	8.1	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods. This can allow a user with access to execute commands in a running Pod to elevate their user privileges. **CVE ID: CVE-2022-43915**	https://exchange.xforce.ibmcloud.com/vulnerabilities/241037, https://www.ibm.com/support/pages/node/7166463	A-IBM-APP_-030924/165
Product: cloud_pak_for_security					
Affected Version(s): From (including) 1.10.0.0 Up to (including) 1.10.11.0					
Generation of Error Message Containing Sensitive Information	16-Aug-2024	7.5	IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the request. This information could be used in further attacks against the system. IBM X-Force ID: 272201.	https://www.ibm.com/support/pages/node/7161427	A-IBM-CLOU-030924/166

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-47728		
Product: global_configuration_management					
Affected Version(s): 7.0.2					
N/A	20-Aug-2024	6.5	IBM Global Configuration Management 7.0.2 and 7.0.3 could allow an authenticated user to archive a global baseline due to improper access controls. **CVE ID: CVE-2024-41773**	https://www.ibm.com/support/pages/node/7165963	A-IBM-GLOB-030924/167
Affected Version(s): 7.0.3					
N/A	20-Aug-2024	6.5	IBM Global Configuration Management 7.0.2 and 7.0.3 could allow an authenticated user to archive a global baseline due to improper access controls. **CVE ID: CVE-2024-41773**	https://www.ibm.com/support/pages/node/7165963	A-IBM-GLOB-030924/168
Product: openpages_grc_platform					
Affected Version(s): 8.3					
Missing Authentication for Critical Function	22-Aug-2024	6.5	IBM OpenPages with Watson 8.3 and 9.0 could allow authenticated users access to sensitive information through improper authorization controls on APIs.	https://www.ibm.com/support/pages/node/7165959	A-IBM-OPEN-030924/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35151		
Product: openpages_with_watson					
Affected Version(s): 9.0					
Missing Authentication for Critical Function	22-Aug-2024	6.5	IBM OpenPages with Watson 8.3 and 9.0 could allow authenticated users access to sensitive information through improper authorization controls on APIs. **CVE ID: CVE-2024-35151**	https://www.ibm.com/support/pages/node/7165959	A-IBM-OPEN-030924/170
Product: qradar_suite					
Affected Version(s): From (including) 1.10.12.0 Up to (excluding) 1.10.23.0					
Generation of Error Message Containing Sensitive Information	16-Aug-2024	7.5	IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the request. This information could be used in further attacks against the system. IBM X-Force ID: 272201. **CVE ID: CVE-2023-47728**	https://www.ibm.com/support/pages/node/7161427	A-IBM-QRAD-030924/171
Product: security_directory_integrator					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.2.0					
N/A	16-Aug-2024	9.8	IBM Security Directory Integrator 7.2.0 and Security Verify Directory Integrator 10.0.0 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. IBM X-Force ID: 228570. **CVE ID: CVE-2022-33162**	https://www.ibm.com/support/pages/node/7161442	A-IBM-SECU-030924/172
Product: security_verify_directory_integrator					
Affected Version(s): 10.0.0					
N/A	16-Aug-2024	9.8	IBM Security Directory Integrator 7.2.0 and Security Verify Directory Integrator 10.0.0 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. IBM X-Force ID: 228570. **CVE ID: CVE-2022-33162**	https://www.ibm.com/support/pages/node/7161442	A-IBM-SECU-030924/173

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sterling_connect_direct_web_services					
Affected Version(s): 6.3.0					
Use of a Broken or Risky Cryptographic Algorithm	22-Aug-2024	7.5	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-39745**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297312, https://www.ibm.com/support/pages/node/7166195	A-IBM-STER-030924/174
Missing Encryption of Sensitive Data	22-Aug-2024	5.9	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **CVE ID: CVE-2024-39746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297313, https://www.ibm.com/support/pages/node/7166018	A-IBM-STER-030924/175
Cross-Site Request Forgery (CSRF)	22-Aug-2024	4.3	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-	https://exchange.xforce.ibmcloud.com/vulnerabilities/297236, https://www.ib	A-IBM-STER-030924/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID: CVE-2024-39744**	m.com/support/pages/node/7166196	
Affected Version(s): 6.0					
Use of a Broken or Risky Cryptographic Algorithm	22-Aug-2024	7.5	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-39745**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297312, https://www.ibm.com/support/pages/node/7166195	A-IBM-STER-030924/177
Missing Encryption of Sensitive Data	22-Aug-2024	5.9	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using	https://exchange.xforce.ibmcloud.com/vulnerabilities/297313, https://www.ibm.com/support/pages/node/7166018	A-IBM-STER-030924/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man in the middle techniques. **CVE ID: CVE-2024-39746**		
Cross-Site Request Forgery (CSRF)	22-Aug-2024	4.3	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID: CVE-2024-39744**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297236, https://www.ibm.com/support/pages/node/7166196	A-IBM-STER-030924/179
Affected Version(s): 6.1.0					
Use of a Broken or Risky Cryptographic Algorithm	22-Aug-2024	7.5	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-39745**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297312, https://www.ibm.com/support/pages/node/7166195	A-IBM-STER-030924/180
Missing Encryption of Sensitive Data	22-Aug-2024	5.9	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information,	https://exchange.xforce.ibmcloud.com/vulnerabilities/297313, https://www.ibm.com/support	A-IBM-STER-030924/181

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **CVE ID: CVE-2024-39746**	/pages/node/7166018	
Cross-Site Request Forgery (CSRF)	22-Aug-2024	4.3	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID: CVE-2024-39744**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297236, https://www.ibm.com/support/pages/node/7166196	A-IBM-STER-030924/182
Affected Version(s): 6.2.0					
Use of a Broken or Risky Cryptographic Algorithm	22-Aug-2024	7.5	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	https://exchange.xforce.ibmcloud.com/vulnerabilities/297312, https://www.ibm.com/support/pages/node/7166195	A-IBM-STER-030924/183

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-39745		
Missing Encryption of Sensitive Data	22-Aug-2024	5.9	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **CVE ID: CVE-2024-39746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297313, https://www.ibm.com/support/pages/node/7166018	A-IBM-STER-030924/184
Cross-Site Request Forgery (CSRF)	22-Aug-2024	4.3	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID: CVE-2024-39744**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297236, https://www.ibm.com/support/pages/node/7166196	A-IBM-STER-030924/185
Vendor: in2code					
Product: powermail					
Affected Version(s): * Up to (excluding) 7.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	29-Aug-2024	9.8	An issue was discovered in powermail extension through 12.3.5 for TYPO3. Several actions in the OutputController can directly be called, due to missing or insufficiently implemented access checks, resulting in Broken Access Control. Depending on the configuration of the Powermail Frontend plugins, an unauthenticated attacker can exploit this to edit, update, delete, or export data of persisted forms. This can only be exploited when the Powermail Frontend plugins are used. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0. **CVE ID: CVE-2024-45233**	N/A	A-IN2-POWE-030924/186
Authorization Bypass Through User-Controlled Key	29-Aug-2024	5.3	An issue was discovered in powermail extension through 12.3.5 for TYPO3. It fails to validate the mail parameter of	N/A	A-IN2-POWE-030924/187

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the confirmationAction, resulting in Insecure Direct Object Reference (IDOR). An unauthenticated attacker can use this to display the user-submitted data of all forms persisted by the extension. This can only be exploited when the extension is configured to save submitted form data to the database (plugin.tx_powermail.settings.db.enable=1), which however is the default setting of the extension. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0 **CVE ID: CVE-2024-45232**		
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.4.0					
N/A	29-Aug-2024	9.8	An issue was discovered in powermail extension through 12.3.5 for TYPO3. Several actions in the OutputController can directly be called, due to missing or insufficiently	N/A	A-IN2-POWE-030924/188

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implemented access checks, resulting in Broken Access Control. Depending on the configuration of the Powermail Frontend plugins, an unauthenticated attacker can exploit this to edit, update, delete, or export data of persisted forms. This can only be exploited when the Powermail Frontend plugins are used. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0. **CVE ID: CVE-2024-45233**		
Authorization Bypass Through User-Controlled Key	29-Aug-2024	5.3	An issue was discovered in powermail extension through 12.3.5 for TYPO3. It fails to validate the mail parameter of the confirmationAction , resulting in Insecure Direct Object Reference (IDOR). An unauthenticated attacker can use this to display the user-submitted data of all forms persisted by the	N/A	A-IN2-POWE-030924/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			extension. This can only be exploited when the extension is configured to save submitted form data to the database (plugin.tx_powermail.settings.db.enable=1), which however is the default setting of the extension. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0 **CVE ID: CVE-2024-45232**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.5.0					
N/A	29-Aug-2024	9.8	An issue was discovered in powermail extension through 12.3.5 for TYPO3. Several actions in the OutputController can directly be called, due to missing or insufficiently implemented access checks, resulting in Broken Access Control. Depending on the configuration of the Powermail Frontend plugins, an unauthenticated attacker can exploit this to edit, update, delete, or export	N/A	A-IN2-POWE-030924/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data of persisted forms. This can only be exploited when the Powermail Frontend plugins are used. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0. **CVE ID: CVE-2024-45233**		
Authorization Bypass Through User-Controlled Key	29-Aug-2024	5.3	An issue was discovered in powermail extension through 12.3.5 for TYPO3. It fails to validate the mail parameter of the confirmationAction, resulting in Insecure Direct Object Reference (IDOR). An unauthenticated attacker can use this to display the user-submitted data of all forms persisted by the extension. This can only be exploited when the extension is configured to save submitted form data to the database (plugin.tx_powermail.settings.db.enable=1), which however is the default setting of	N/A	A-IN2-POWE-030924/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the extension. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0 **CVE ID: CVE-2024-45232**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 10.9.0					
N/A	29-Aug-2024	9.8	An issue was discovered in powermail extension through 12.3.5 for TYPO3. Several actions in the OutputController can directly be called, due to missing or insufficiently implemented access checks, resulting in Broken Access Control. Depending on the configuration of the Powermail Frontend plugins, an unauthenticated attacker can exploit this to edit, update, delete, or export data of persisted forms. This can only be exploited when the Powermail Frontend plugins are used. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0.	N/A	A-IN2-POWE-030924/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45233		
Authorization Bypass Through User-Controlled Key	29-Aug-2024	5.3	An issue was discovered in powermail extension through 12.3.5 for TYPO3. It fails to validate the mail parameter of the confirmationAction, resulting in Insecure Direct Object Reference (IDOR). An unauthenticated attacker can use this to display the user-submitted data of all forms persisted by the extension. This can only be exploited when the extension is configured to save submitted form data to the database (plugin.tx_powermail.settings.db.enable=1), which however is the default setting of the extension. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0 **CVE ID: CVE-2024-45232**	N/A	A-IN2-POWE-030924/193
Vendor: innocms					
Product: innocms					
Affected Version(s): 0.3.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	17-Aug-2024	7.2	A vulnerability, which was classified as critical, has been found in InnoCMS 0.3.1. This issue affects some unknown processing of the file /panel/pages/1/edit of the component Backend. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7899**	N/A	A-INN-INNO-030924/194
Vendor: insurance_management_system_project					
Product: insurance_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-2024	6.1	A vulnerability has been found in nafisulbari/itsourcecode Insurance Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown	N/A	A-INS-INSU-030924/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality of the file editClient.php. The manipulation of the argument AGENT ID leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8208**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-2024	6.1	A vulnerability was found in nafisulbari/itsourcecode Insurance Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file addClient.php. The manipulation of the argument CLIENT ID leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The	N/A	A-INS-INSU-030924/196

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8209**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-2024	5.4	A vulnerability classified as problematic was found in nafisulbari/itsourcecode Insurance Management System 1.0. Affected by this vulnerability is an unknown functionality of the file addNominee.php of the component Add Nominee Page. The manipulation of the argument Nominee-Client ID leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7916**	N/A	A-INS-INSU-030924/197

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Aug-2024	5.4	A vulnerability, which was classified as critical, has been found in nafisulbari/itsourcecode Insurance Management System 1.0. Affected by this issue is some unknown functionality of the file editPayment.php of the component Payment Handler. The manipulation of the argument recipt_no leads to improper access controls. The attack may be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8216**	N/A	A-INS-INSU-030924/198
Vendor: Irfanview					
Product: irfanview					
Affected Version(s): 4.67					
Out-of-bounds Write	21-Aug-2024	7.8	IrfanView WSQ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote	N/A	A-IRF-IRFA-030924/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WSQ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24192. **CVE ID: CVE-2024-6811**		
Out-of-bounds Write	21-Aug-2024	7.8	IrfanView WSQ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to	N/A	A-IRF-IRFA-030924/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WSQ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23273. **CVE ID: CVE-2024-6812**		
Affected Version(s): 4.67.1.0					
N/A	28-Aug-2024	5.5	An issue in the component EXR!ReadEXR+0x40ef1 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR	N/A	A-IRF-IRFA-030924/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file. This vulnerability can lead to a Denial of Service (DoS). **CVE ID: CVE-2024-44913**		
N/A	28-Aug-2024	5.5	An issue in the component EXR!ReadEXR+0x3df50 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS). **CVE ID: CVE-2024-44914**	N/A	A-IRF-IRFA-030924/202
N/A	28-Aug-2024	5.5	An issue in the component EXR!ReadEXR+0x4eef0 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS). **CVE ID: CVE-2024-44915**	N/A	A-IRF-IRFA-030924/203
Product: wsq					
Affected Version(s): 2024.02.16					
Out-of-bounds Write	21-Aug-2024	7.8	IrfanView WSQ File Parsing Out-Of-Bounds Write Remote Code Execution	N/A	A-IRF-WSQ-030924/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WSQ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24192. **CVE ID: CVE-2024-6811**		
Out-of-bounds Write	21-Aug-2024	7.8	IrfanView WSQ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This	N/A	A-IRF-WSQ-030924/205

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WSQ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23273. **CVE ID: CVE-2024-6812**		
Vendor: janobe					
Product: e-commerce_system					
Affected Version(s): 1.0					
Improper Neutralization of	22-Aug-2024	9.8	A vulnerability has been found in SourceCodester E-	N/A	A-JAN-E-CO-030924/206

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Commerce System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ecommerce/admin/login.php of the component Admin Login. The manipulation of the argument user_email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8086**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Aug-2024	9.8	A vulnerability was found in SourceCodester E-Commerce System 1.0 and classified as critical. This issue affects some unknown processing of the file /ecommerce/popup_Item.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.	N/A	A-JAN-E-CO-030924/207

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8087		
Unrestricted Upload of File with Dangerous Type	23-Aug-2024	9.8	A vulnerability was found in SourceCodester E-Commerce System 1.0. It has been classified as critical. Affected is an unknown function of the file /ecommerce/admin/products/controller.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8089**	N/A	A-JAN-E-CO-030924/208
Product: point_of_sales_and_inventory_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	9.8	A vulnerability classified as critical has been found in SourceCodester Point of Sales and Inventory Management System 1.0. This affects an unknown part of the file login.php. The manipulation of the	N/A	A-JAN-POIN-030924/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7947**		
Vendor: Jetbrains					
Product: teamcity					
Affected Version(s): * Up to (excluding) 2024.07.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-2024	6.1	In JetBrains TeamCity before 2024.07.1 reflected XSS was possible on the agentPushPreset page **CVE ID: CVE-2024-43809**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-030924/210
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-2024	5.4	In JetBrains TeamCity before 2024.07.1 multiple stored XSS was possible on Clouds page **CVE ID: CVE-2024-43807**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-030924/211
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-2024	5.4	In JetBrains TeamCity before 2024.07.1 self XSS was possible in the HashiCorp Vault plugin **CVE ID: CVE-2024-43808**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-030924/212

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Aug-2024	5.4	In JetBrains TeamCity before 2024.07.1 reflected XSS was possible in the AWS Core plugin **CVE ID: CVE-2024-43810**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-030924/213
Vendor: jielink\+_jsotc2016_project					
Product: jielink\+_jsotc2016					
Affected Version(s): * Up to (including) 20240805					
N/A	19-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in Anhui Deshun Intelligent Technology Jieshun JieLink+ JSOTC2016 up to 20240805. This issue affects some unknown processing of the file /report/ParkChargeRecord/GetDataList. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7919**	N/A	A-JIE-JIEL-030924/214
N/A	19-Aug-2024	9.8	A vulnerability, which was classified as	N/A	A-JIE-JIEL-030924/215

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic, was found in Anhui Deshun Intelligent Technology Jieshun JieLink+ JSOTC2016 up to 20240805. Affected is an unknown function of the file /Report/ParkCommon/GetParkInThroughDeivces. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7920**		
N/A	19-Aug-2024	9.8	A vulnerability has been found in Anhui Deshun Intelligent Technology Jieshun JieLink+ JSOTC2016 up to 20240805 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /report/ParkOutRecord/GetDataList. The manipulation leads to improper	N/A	A-JIE-JIEL-030924/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7921**		
Vendor: jkev					
Product: record_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Aug-2024	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Record Management System 1.0. This affects an unknown part of the file sort1_user.php. The manipulation of the argument position 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. **CVE ID: CVE-2024-8136**	N/A	A-JKE-RECO-030924/217
Improper Neutralization of Input During Web Page	24-Aug-2024	6.1	A vulnerability has been found in SourceCodester Record Management	N/A	A-JKE-RECO-030924/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			System 1.0 and classified as problematic. This vulnerability affects unknown code of the file search_user.php. The manipulation of the argument search leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8137**		
Vendor: Jupyter					
Product: jupyterlab					
Affected Version(s): * Up to (excluding) 3.6.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Aug-2024	6.1	jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. This vulnerability depends on user interaction by opening a malicious notebook with Markdown cells, or Markdown file using JupyterLab preview feature. A malicious user can access any data that	https://github.com/jupyterlab/jupyterlab/security/advisories/GHSA-9q39-rmj3-p4r2	A-JUP-JUPY-030924/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab v3.6.8, v4.2.5 and Jupyter Notebook v7.2.2 have been patched to resolve this issue. Users are advised to upgrade. There is no workaround for the underlying DOM Clobbering susceptibility. However, select plugins can be disabled on deployments which cannot update in a timely fashion to minimise the risk. These are: 1. `@jupyterlab/mathjax-extension:plugin` - users will loose ability to preview mathematical equations. 2. `@jupyterlab/markdownviewer-extension:plugin` - users will loose ability to open Markdown previews. 3. `@jupyterlab/mathjax2-extension:plugin` (if installed with		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			optional `jupyterlab-mathjax2` package) - an older version of the mathjax plugin for JupyterLab 4.x. To disable these extensions run: ```jupyter labextension disable @jupyterlab/markdownviewer-extension:plugin && jupyter labextension disable @jupyterlab/mathjax-extension:plugin && jupyter labextension disable @jupyterlab/mathjax2-extension:plugin ``` in bash. **CVE ID: CVE-2024-43805**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Aug-2024	6.1	jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. This vulnerability depends on user interaction by opening a malicious	https://github.com/jupyterlab/jupyterlab/security/advisories/GHSA-9q39-rmj3-p4r2	A-JUP-JUPY-030924/220

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			notebook with Markdown cells, or Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab v3.6.8, v4.2.5 and Jupyter Notebook v7.2.2 have been patched to resolve this issue. Users are advised to upgrade. There is no workaround for the underlying DOM Clobbering susceptibility. However, select plugins can be disabled on deployments which cannot update in a timely fashion to minimise the risk. These are: 1. `@jupyterlab/mathjax-extension:plugin` - users will loose ability to preview mathematical equations. 2. `@jupyterlab/markdownviewer-extension:plugin` - users will loose		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to open Markdown previews. 3. `@jupyterlab/mathjax2-extension:plugin` (if installed with optional `jupyterlab-mathjax2` package) - an older version of the mathjax plugin for JupyterLab 4.x. To disable these extensions run: ```jupyter labextension disable @jupyterlab/markdownviewer-extension:plugin && jupyter labextension disable @jupyterlab/mathjax-extension:plugin && jupyter labextension disable @jupyterlab/mathjax2-extension:plugin ``` in bash. **CVE ID: CVE-2024-43805**		
Product: notebook					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.2.2					
Improper Neutralization of Input During Web Page	28-Aug-2024	6.1	jupyterlab is an extensible environment for interactive and reproducible	https://github.com/jupyterlab/jupyterlab/security/advisories/	A-JUP-NOTE-030924/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			computing, based on the Jupyter Notebook Architecture. This vulnerability depends on user interaction by opening a malicious notebook with Markdown cells, or Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab v3.6.8, v4.2.5 and Jupyter Notebook v7.2.2 have been patched to resolve this issue. Users are advised to upgrade. There is no workaround for the underlying DOM Clobbering susceptibility. However, select plugins can be disabled on deployments which cannot update in a timely fashion to minimise the risk. These are: 1. `@jupyterlab/mathjax-extension:plugin` -	GHSA-9q39-rmj3-p4r2	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	users will loose ability to preview mathematical equations. 2. `@jupyterlab/markdownviewer-extension:plugin` - users will loose ability to open Markdown previews. 3. `@jupyterlab/mathjax2-extension:plugin` (if installed with optional `jupyterlab-mathjax2` package) - an older version of the mathjax plugin for JupyterLab 4.x. To disable these extensions run: ```jupyter labextension disable @jupyterlab/markdownviewer-extension:plugin && jupyter labextension disable @jupyterlab/mathjax-extension:plugin && jupyter labextension disable @jupyterlab/mathjax2-extension:plugin ``` in bash.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43805		
Vendor: kevinwong					
Product: payroll_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Aug-2024	9.8	A vulnerability classified as critical was found in itsourcecode Payroll Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8081**	N/A	A-KEV-PAYR-030924/222
Vendor: keyfactor					
Product: aws_orchestrator					
Affected Version(s): * Up to (excluding) 2.01					
N/A	20-Aug-2024	7.5	Keyfactor AWS Orchestrator through 2.0 allows Information Disclosure. **CVE ID: CVE-2024-42006**	https://trust.keyfactor.com/?itemUid=d73921fd-bc9e-4e35-a974-cfb628e6a226&source=click	A-KEY-AWS_-030924/223
Product: command					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	7.5	Keyfactor Command 10.5.x before 10.5.1 and 11.5.x before 11.5.1 allows SQL Injection which could result in information disclosure. **CVE ID: CVE-2024-34458**	https://trust.keyfactor.com/?itemUid=d73921fd-bc9e-4e35-a974-cfb628e6a226&source=click	A-KEY-COMM-030924/224
Affected Version(s): 11.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	7.5	Keyfactor Command 10.5.x before 10.5.1 and 11.5.x before 11.5.1 allows SQL Injection which could result in information disclosure. **CVE ID: CVE-2024-34458**	https://trust.keyfactor.com/?itemUid=d73921fd-bc9e-4e35-a974-cfb628e6a226&source=click	A-KEY-COMM-030924/225
Vendor: kitsada8621					
Product: digital_library_management_system					
Affected Version(s): 1.0					
Improper Encoding or Escaping of Output	29-Aug-2024	7.5	A vulnerability was found in kitsada8621 Digital Library Management System 1.0. It has been classified as problematic. Affected is the function JwtRefreshAuth of the file middleware/jwt_refresh_token_middle	https://github.com/kitsada8621/Digital-Library-Management-System/commit/81b3336b4c9240f0bf50c13cb8375cf860d945f1	A-KIT-DIGI-030924/226

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ware.go. The manipulation of the argument Authorization leads to improper output neutralization for logs. It is possible to launch the attack remotely. The name of the patch is 81b3336b4c9240f0bf50c13cb8375cf860d945f1. It is recommended to apply a patch to fix this issue. **CVE ID: CVE-2024-8297**		
Vendor: kjayvik					
Product: bus_ticket_reservation_system					
Affected Version(s): 1.0					
N/A	23-Aug-2024	5.4	Kashipara Bus Ticket Reservation System v1.0 0 is vulnerable to Incorrect Access Control via /deleteTicket.php. **CVE ID: CVE-2024-42766**	N/A	A-KJA-BUS_-030924/227
Vendor: lfedge					
Product: ekuiper					
Affected Version(s): * Up to (excluding) 1.14.2					
Improper Neutralization of Special Elements used in an SQL	20-Aug-2024	8.8	LF Edge eKuiper is a lightweight IoT data analytics and stream processing engine running on resource-constraint edge	https://github.com/lf-edge/ekuiper/commit/1a9c745649438feaac357d282959687012b65503,	A-LFE-EKUI-030924/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			devices. A user could utilize and exploit SQL Injection to allow the execution of malicious SQL query via Get method in sqlKvStore. This vulnerability is fixed in 1.14.2. **CVE ID: CVE-2024-43406**	https://github.com/lf-edge/ekuiper/security/advisories/GHSA-r5ph-4jxm-6j9p	
Vendor: logsign					
Product: unified_secops_platform					
Affected Version(s): 6.4.20					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-2024	8.1	Logsign Unified SecOps Platform Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper	N/A	A-LOG-UNIF-030924/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of root. Was ZDI-CAN-25025. **CVE ID: CVE-2024-7600**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-2024	8.1	Logsign Unified SecOps Platform Directory data_export_delete_all Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file	N/A	A-LOG-UNIF-030924/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operations. An attacker can leverage this vulnerability to delete files in the context of root. Was ZDI-CAN-25026. **CVE ID: CVE-2024-7601**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-2024	8.1	Logsign Unified SecOps Platform Directory Traversal Arbitrary Directory Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary directories on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to	N/A	A-LOG-UNIF-030924/231

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete directories in the context of root. Was ZDI-CAN-25028. **CVE ID: CVE-2024-7603**		
Incorrect Authorization	21-Aug-2024	7.8	Logsign Unified SecOps Platform Incorrect Authorization Authentication Bypass Vulnerability. This vulnerability allows local attackers to bypass authentication on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of the user's license expiration date. An attacker can leverage this vulnerability to bypass authentication on	N/A	A-LOG-UNIF-030924/232

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the system. Was ZDI-CAN-25029. **CVE ID: CVE-2024-7604**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-2024	6.5	Logsign Unified SecOps Platform Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Logsign Unified SecOps Platform. Authentication is required to exploit this vulnerability. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-25027.	N/A	A-LOG-UNIF-030924/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7602		
Vendor: lopalopa					
Product: music_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	21-Aug-2024	9.8	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=signup" of Kashipara Music Management System v1.0, which allows attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID: CVE-2024-42777**	N/A	A-LOP-MUSI-030924/234
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Aug-2024	9.8	A SQL injection vulnerability in "/music/ajax.php?action=login" of Kashipara Music Management System v1.0 allows remote attackers to execute arbitrary SQL commands and bypass Login via the email parameter. **CVE ID: CVE-2024-42781**	N/A	A-LOP-MUSI-030924/235
Improper Neutralization of Special Elements used in an	21-Aug-2024	9.8	A SQL injection vulnerability in "/music/ajax.php?action=find_music" in Kashipara Music Management	N/A	A-LOP-MUSI-030924/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			System v1.0 allows an attacker to execute arbitrary SQL commands via the "search" parameter. **CVE ID: CVE-2024-42782**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Aug-2024	9.8	A SQL injection vulnerability in "/music/controller.php?page=view_music" in Kashipara Music Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "id" parameter. **CVE ID: CVE-2024-42784**	N/A	A-LOP-MUSI-030924/237
Unrestricted Upload of File with Dangerous Type	21-Aug-2024	8.8	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_playlist" in Kashipara Music Management System v1.0. This allows attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID: CVE-2024-42778**	N/A	A-LOP-MUSI-030924/238
Unrestricted Upload of File with Dangerous Type	21-Aug-2024	8.8	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_music	N/A	A-LOP-MUSI-030924/239

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			" in Kashipara Music Management System v1.0. This allows attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID: CVE-2024-42779**		
Unrestricted Upload of File with Dangerous Type	21-Aug-2024	8.8	An Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_genre" in Kashipara Music Management System v1.0. This allows attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID: CVE-2024-42780**	N/A	A-LOP-MUSI-030924/240
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Aug-2024	8.8	A SQL injection vulnerability in /music/index.php?page=view_playlist in Kashipara Music Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "id" parameter. **CVE ID: CVE-2024-42785**	N/A	A-LOP-MUSI-030924/241
Improper Neutralization of Special Elements	21-Aug-2024	8.8	A SQL injection vulnerability in "/music/view_user.php" in Kashipara Music Management	N/A	A-LOP-MUSI-030924/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			System v1.0 allows an attacker to execute arbitrary SQL commands via the "id" parameter of View User Profile Page. **CVE ID: CVE-2024-42786**		
Cross-Site Request Forgery (CSRF)	28-Aug-2024	8	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Music Management System v1.0 via a crafted request to the /music/ajax.php?action=save_user page. **CVE ID: CVE-2024-42793**	N/A	A-LOP-MUSI-030924/243
Product: responsive_school_management_system					
Affected Version(s): 3.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Aug-2024	7.2	A SQL injection vulnerability in /smsa/admin_login.php in Kashipara Responsive School Management System v3.2.0 allows an attacker to execute arbitrary SQL commands via the "username" parameter of the Admin Login Page **CVE ID: CVE-2024-41236**	N/A	A-LOP-RESP-030924/244
Vendor: magnetforensics					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: axiom					
Affected Version(s): 8.0.0.39753					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-2024	8	Magnet Forensics AXIOM Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Magnet Forensics AXIOM. User interaction is required to exploit this vulnerability in that the target must acquire data from a malicious mobile device. The specific flaw exists within the Android device image acquisition functionality. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-23964.	N/A	A-MAG-AXIO-030924/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7448		
Vendor: Matrix					
Product: javascript_sdk					
Affected Version(s): * Up to (excluding) 34.3.1					
Uncontrolled Recursion	20-Aug-2024	5.3	matrix-js-sdk is a Matrix messaging protocol Client-Server SDK for JavaScript. A malicious homeserver can craft a room or room structure such that the predecessors form a cycle. The matrix-js-sdk's getRoomUpgradeHistory function will infinitely recurse in this case, causing the code to hang. This method is public but also called by the 'leaveRoomChain()' method, so leaving a room will also trigger the bug. This was patched in matrix-js-sdk 34.3.1. **CVE ID: CVE-2024-42369**	https://github.com/matrix-org/matrix-js-sdk/commit/a0efed8b881b3db6c9f2c71d6a6e74c2828978c6, https://github.com/matrix-org/matrix-js-sdk/security/advisories/GHSA-vhr5-g3pm-49fm	A-MAT-JAVA-030924/246
Vendor: mattermost					
Product: mattermost					
Affected Version(s): From (including) 9.10.0 Up to (excluding) 9.10.1					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	22-Aug-2024	8.8	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to sanitize user inputs in the frontend that are used for redirection which allows for a one-click client-side path traversal that is leading to CSRF in User Management page of the system console. **CVE ID: CVE-2024-40886**	https://mattermost.com/security-updates	A-MAT-MATT-030924/247
N/A	22-Aug-2024	7.2	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to restrict which roles can promote a user as system admin which allows a System Role with edit access to the permissions section of system console to update their role (e.g. member) to include the `manage_system` permission, effectively becoming a System Admin. **CVE ID: CVE-2024-8071**	https://mattermost.com/security-updates	A-MAT-MATT-030924/248

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Aug-2024	6.5	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to ensure that remote/synthetic users cannot create sessions or reset passwords, which allows the munged email addresses, created by shared channels, to be used to receive email notifications and to reset passwords, when they are valid, functional emails. **CVE ID: CVE-2024-39836**	https://mattermost.com/security-updates	A-MAT-MATT-030924/249
Improper Check for Unusual or Exceptional Conditions	22-Aug-2024	5.3	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to restrict the input in POST /api/v4/users which allows a user to manipulate the creation date in POST /api/v4/users tricking the admin into believing their account is much older. **CVE ID: CVE-2024-42411**	https://mattermost.com/security-updates	A-MAT-MATT-030924/250

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Aug-2024	4.9	Mattermost versions 9.5.x <= 9.5.7 and 9.10.x <= 9.10.0 fail to time limit and size limit the CA path file in the ElasticSearch configuration which allows a System Role with access to the Elasticsearch system console to add any file as a CA path field, such as /dev/zero and, after testing the connection, cause the application to crash. **CVE ID: CVE-2024-39810**	https://mattermost.com/security-updates	A-MAT-MATT-030924/251
N/A	22-Aug-2024	4.3	Mattermost versions 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 fail to enforce proper access controls which allows any authenticated user, including guests, to mark any channel inside any team as read for any user. **CVE ID: CVE-2024-43813**	https://mattermost.com/security-updates	A-MAT-MATT-030924/252
Cleartext Storage of Sensitive Information	22-Aug-2024	3.7	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2, when shared channels are enabled, fail to	https://mattermost.com/security-updates	A-MAT-MATT-030924/253

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			redact remote users' original email addresses stored in user props when email addresses are otherwise configured not to be visible in the local server." **CVE ID: CVE-2024-32939**		
Affected Version(s): From (including) 9.5.0 Up to (excluding) 9.5.8					
Cross-Site Request Forgery (CSRF)	22-Aug-2024	8.8	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to sanitize user inputs in the frontend that are used for redirection which allows for a one-click client-side path traversal that is leading to CSRF in User Management page of the system console. **CVE ID: CVE-2024-40886**	https://mattermost.com/security-updates	A-MAT-MATT-030924/254
N/A	22-Aug-2024	7.2	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to restrict which roles can promote a user as system admin which allows a System Role with	https://mattermost.com/security-updates	A-MAT-MATT-030924/255

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			edit access to the permissions section of system console to update their role (e.g. member) to include the `manage_system` permission, effectively becoming a System Admin. **CVE ID: CVE-2024-8071**		
N/A	22-Aug-2024	6.5	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to ensure that remote/synthetic users cannot create sessions or reset passwords, which allows the munged email addresses, created by shared channels, to be used to receive email notifications and to reset passwords, when they are valid, functional emails. **CVE ID: CVE-2024-39836**	https://mattermost.com/security-updates	A-MAT-MATT-030924/256
Improper Check for Unusual or Exceptiona	22-Aug-2024	5.3	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to restrict the input in	https://mattermost.com/security-updates	A-MAT-MATT-030924/257

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			POST /api/v4/users which allows a user to manipulate the creation date in POST /api/v4/users tricking the admin into believing their account is much older. **CVE ID: CVE-2024-42411**		
N/A	22-Aug-2024	4.9	Mattermost versions 9.5.x <= 9.5.7 and 9.10.x <= 9.10.0 fail to time limit and size limit the CA path file in the ElasticSearch configuration which allows a System Role with access to the Elasticsearch system console to add any file as a CA path field, such as /dev/zero and, after testing the connection, cause the application to crash. **CVE ID: CVE-2024-39810**	https://mattermost.com/security-updates	A-MAT-MATT-030924/258
N/A	22-Aug-2024	4.3	Mattermost versions 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 fail to enforce proper access controls which allows any authenticated user,	https://mattermost.com/security-updates	A-MAT-MATT-030924/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including guests, to mark any channel inside any team as read for any user. **CVE ID: CVE-2024-43813**		
Cleartext Storage of Sensitive Information	22-Aug-2024	3.7	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2, when shared channels are enabled, fail to redact remote users' original email addresses stored in user props when email addresses are otherwise configured not to be visible in the local server." **CVE ID: CVE-2024-32939**	https://mattermost.com/security-updates	A-MAT-MATT-030924/260
Affected Version(s): From (including) 9.8.0 Up to (excluding) 9.8.3					
Cross-Site Request Forgery (CSRF)	22-Aug-2024	8.8	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to sanitize user inputs in the frontend that are used for redirection which allows for a one-click client-side path traversal that is leading to CSRF in User Management page	https://mattermost.com/security-updates	A-MAT-MATT-030924/261

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the system console. **CVE ID: CVE-2024-40886**		
N/A	22-Aug-2024	7.2	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to restrict which roles can promote a user as system admin which allows a System Role with edit access to the permissions section of system console to update their role (e.g. member) to include the `manage_system` permission, effectively becoming a System Admin. **CVE ID: CVE-2024-8071**	https://mattermost.com/security-updates	A-MAT-MATT-030924/262
N/A	22-Aug-2024	6.5	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to ensure that remote/synthetic users cannot create sessions or reset passwords, which allows the munged email addresses, created by shared channels, to be used to receive	https://mattermost.com/security-updates	A-MAT-MATT-030924/263

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			email notifications and to reset passwords, when they are valid, functional emails. **CVE ID: CVE-2024-39836**		
Improper Check for Unusual or Exceptional Conditions	22-Aug-2024	5.3	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to restrict the input in POST /api/v4/users which allows a user to manipulate the creation date in POST /api/v4/users tricking the admin into believing their account is much older. **CVE ID: CVE-2024-42411**	https://mattermost.com/security-updates	A-MAT-MATT-030924/264
Cleartext Storage of Sensitive Information	22-Aug-2024	3.7	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2, when shared channels are enabled, fail to redact remote users' original email addresses stored in user props when email addresses are otherwise configured not to	https://mattermost.com/security-updates	A-MAT-MATT-030924/265

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be visible in the local server." **CVE ID: CVE-2024-32939**		
Affected Version(s): From (including) 9.9.0 Up to (excluding) 9.9.2					
Cross-Site Request Forgery (CSRF)	22-Aug-2024	8.8	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to sanitize user inputs in the frontend that are used for redirection which allows for a one-click client-side path traversal that is leading to CSRF in User Management page of the system console. **CVE ID: CVE-2024-40886**	https://mattermost.com/security-updates	A-MAT-MATT-030924/266
N/A	22-Aug-2024	7.2	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to restrict which roles can promote a user as system admin which allows a System Role with edit access to the permissions section of system console to update their role (e.g. member) to include the `manage_system`	https://mattermost.com/security-updates	A-MAT-MATT-030924/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission, effectively becoming a System Admin. **CVE ID: CVE-2024-8071**		
N/A	22-Aug-2024	6.5	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0 and 9.8.x <= 9.8.2 fail to ensure that remote/synthetic users cannot create sessions or reset passwords, which allows the munged email addresses, created by shared channels, to be used to receive email notifications and to reset passwords, when they are valid, functional emails. **CVE ID: CVE-2024-39836**	https://mattermost.com/security-updates	A-MAT-MATT-030924/268
Improper Check for Unusual or Exceptional Conditions	22-Aug-2024	5.3	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2 fail to restrict the input in POST /api/v4/users which allows a user to manipulate the creation date in POST /api/v4/users tricking the admin	https://mattermost.com/security-updates	A-MAT-MATT-030924/269

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into believing their account is much older. **CVE ID: CVE-2024-42411**		
Cleartext Storage of Sensitive Information	22-Aug-2024	3.7	Mattermost versions 9.9.x <= 9.9.1, 9.5.x <= 9.5.7, 9.10.x <= 9.10.0, 9.8.x <= 9.8.2, when shared channels are enabled, fail to redact remote users' original email addresses stored in user props when email addresses are otherwise configured not to be visible in the local server." **CVE ID: CVE-2024-32939**	https://mattermost.com/security-updates	A-MAT-MATT-030924/270
Vendor: megacord					
Product: megabot					
Affected Version(s): * Up to (excluding) 1.5.0					
Improper Control of Generation of Code ('Code Injection')	20-Aug-2024	9.8	MEGABOT is a fully customized Discord bot for learning and fun. The `/math` command and functionality of MEGABOT versions < 1.5.0 contains a remote code execution vulnerability due to a Python `eval()`. The vulnerability allows an attacker to inject Python	https://github.com/NicPWNs/MEGABOT/commit/71e79e5581ea36313700385b112d863053fb7ed6, https://github.com/NicPWNs/MEGABOT/pull/138, https://github.com/NicPWNs/MEGABOT/security/advisories/	A-MEG-MEGA-030924/271

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code into the `expression` parameter when using `/math` in any Discord channel. This vulnerability impacts any discord guild utilizing MEGABOT. This vulnerability was fixed in release version 1.5.0. **CVE ID: CVE-2024-43404**	GHSA-vhxp-4hwq-w3p2	
Vendor: menulux					
Product: managment_portal					
Affected Version(s): * Up to (including) 21.05.2024					
N/A	29-Aug-2024	9.8	Improper Privilege Management vulnerability in Menulux Information Technologies Managment Portal allows Collect Data as Provided by Users.This issue affects Managment Portal: through 21.05.2024. **CVE ID: CVE-2024-4428**	N/A	A-MEN-MANA-030924/272
Vendor: microcks					
Product: microcks					
Affected Version(s): * Up to (excluding) 1.10.0					
N/A	19-Aug-2024	9.8	In Microcks before 1.10.0, the POST /api/import and POST /api/export	https://github.com/microcks/microcks/compare/1.9.1-fix-	A-MIC-MICR-030924/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints allow non-administrator access. **CVE ID: CVE-2024-44076**	1...1.10.0, https://github.com/microcks/microcks/issues/1212	
Vendor: Microfocus					
Product: netiq_privileged_access_manager					
Affected Version(s): * Up to (excluding) 3.7					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-2024	7.8	SSH authenticated user when access the PAM server can execute an OS command to gain the full system access using bash. This issue affects Privileged Access Manager before 3.7.0.1. **CVE ID: CVE-2020-11847**	N/A	A-MIC-NETI-030924/274
N/A	21-Aug-2024	7.5	A vulnerability found in OpenText Privileged Access Manager that issues a token. on successful issuance of the token, a cookie gets set that allows unrestricted access to all the application resources. This issue affects Privileged Access Manager before 3.7.0.1. **CVE ID: CVE-2020-11846**	N/A	A-MIC-NETI-030924/275
Affected Version(s): 3.7					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Aug-2024	7.8	SSH authenticated user when access the PAM server can execute an OS command to gain the full system access using bash. This issue affects Privileged Access Manager before 3.7.0.1. **CVE ID: CVE-2020-11847**	N/A	A-MIC-NETI-030924/276
N/A	21-Aug-2024	7.5	A vulnerability found in OpenText Privileged Access Manager that issues a token. on successful issuance of the token, a cookie gets set that allows unrestricted access to all the application resources. This issue affects Privileged Access Manager before 3.7.0.1. **CVE ID: CVE-2020-11846**	N/A	A-MIC-NETI-030924/277
Product: netiq_self_service_password_reset					
Affected Version(s): * Up to (excluding) 4.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-2024	6.1	Improper Input Validation vulnerability in OpenText Self Service Password Reset allows Cross-Site Scripting (XSS). This issue affects Self Service	N/A	A-MIC-NETI-030924/278

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Password Reset before 4.5.0.2 and 4.4.0.6 **CVE ID: CVE-2020-11850**		
Affected Version(s): 4.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-2024	6.1	Improper Input Validation vulnerability in OpenText Self Service Password Reset allows Cross-Site Scripting (XSS). This issue affects Self Service Password Reset before 4.5.0.2 and 4.4.0.6 **CVE ID: CVE-2020-11850**	N/A	A-MIC-NETI-030924/279
Affected Version(s): 4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-2024	6.1	Improper Input Validation vulnerability in OpenText Self Service Password Reset allows Cross-Site Scripting (XSS). This issue affects Self Service Password Reset before 4.5.0.2 and 4.4.0.6 **CVE ID: CVE-2020-11850**	N/A	A-MIC-NETI-030924/280
Vendor: Microsoft					
Product: edge					
Affected Version(s): * Up to (excluding) 128.0.2739.42					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Aug-2024	6.1	Microsoft Edge for Android Spoofing Vulnerability **CVE ID: CVE-2024-38208**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38208	A-MIC-EDGE-030924/281
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 128.0.2739.42					
N/A	22-Aug-2024	7.8	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38209**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38209	A-MIC-EDGE-030924/282
N/A	22-Aug-2024	7.8	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID: CVE-2024-38210**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38210	A-MIC-EDGE-030924/283
Out-of-bounds Write	23-Aug-2024	6.3	Microsoft Edge (HTML-based) Memory Corruption Vulnerability **CVE ID: CVE-2024-38207**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38207	A-MIC-EDGE-030924/284
Affected Version(s): * Up to (excluding) 127.0.2651.105					
N/A	16-Aug-2024	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability **CVE ID: CVE-2024-43472**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43472	A-MIC-EDGE-030924/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Mongodb					
Product: mongodb					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.14					
Externally Controlled Reference to a Resource in Another Sphere	27-Aug-2024	6.7	In certain highly specific configurations of the host system and MongoDB server binary installation on Linux Operating Systems, it may be possible for a unintended actor with host-level access to cause the MongoDB Server binary to load unintended actor-controlled shared libraries when the server binary is started, potentially resulting in the unintended actor gaining full control over the MongoDB server process. This issue affects MongoDB Server v5.0 versions prior to 5.0.14 and MongoDB Server v6.0 versions prior to 6.0.3. Required Configuration: Only environments with Linux as the underlying operating system is	https://jira.mongodb.org/browse/SERVER-69507	A-MON-MONG-030924/286

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by this issue **CVE ID: CVE-2024-8207**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.3					
Externally Controlled Reference to a Resource in Another Sphere	27-Aug-2024	6.7	In certain highly specific configurations of the host system and MongoDB server binary installation on Linux Operating Systems, it may be possible for a unintended actor with host-level access to cause the MongoDB Server binary to load unintended actor-controlled shared libraries when the server binary is started, potentially resulting in the unintended actor gaining full control over the MongoDB server process. This issue affects MongoDB Server v5.0 versions prior to 5.0.14 and MongoDB Server v6.0 versions prior to 6.0.3. Required Configuration: Only environments with Linux as the underlying	https://jira.mongodb.org/browse/SERVER-69507	A-MON-MONG-030924/287

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system is affected by this issue **CVE ID: CVE-2024-8207**		
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.1					
Externally Controlled Reference to a Resource in Another Sphere	27-Aug-2024	6.7	In certain highly specific configurations of the host system and MongoDB server binary installation on Linux Operating Systems, it may be possible for a unintended actor with host-level access to cause the MongoDB Server binary to load unintended actor-controlled shared libraries when the server binary is started, potentially resulting in the unintended actor gaining full control over the MongoDB server process. This issue affects MongoDB Server v5.0 versions prior to 5.0.14 and MongoDB Server v6.0 versions prior to 6.0.3. Required Configuration: Only environments with Linux as the	https://jira.mongodb.org/browse/SERVER-69507	A-MON-MONG-030924/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system is affected by this issue **CVE ID: CVE-2024-8207**		
Vendor: Netgear					
Product: prosafe_network_management_system					
Affected Version(s): 1.7.0.34					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Aug-2024	8.8	NETGEAR ProSAFE Network Management System getSortString SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the getSortString method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An	https://kb.netgear.com/000066231/Security-Advisory-for-SQL-Injection-on-the-NMS300-PSV-2024-0018	A-NET-PROS-030924/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-23207. **CVE ID: CVE-2024-6813**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Aug-2024	8.8	NETGEAR ProSAFE Network Management System getFilterString SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the getFilterString method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can	https://kb.netgear.com/000066232/Security-Advisory-for-SQL-Injection-on-the-NMS300-PSV-2024-0019	A-NET-PROS-030924/290

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-23399. **CVE ID: CVE-2024-6814**		
Vendor: newlib_project					
Product: newlib					
Affected Version(s): 4.3.0					
Integer Overflow or Wraparound	20-Aug-2024	9.8	An issue in newlib v.4.3.0 allows an attacker to execute arbitrary code via the time unit scaling in the _gettimeofday function. **CVE ID: CVE-2024-30949**	https://gist.github.com/visitorckw/6b26e599241ea80210ea136b28441661, https://inbox.sourceware.org/newlib/20231129035714.469943-1-visitorckw%40gmail.com/	A-NEW-NEWL-030924/291
Vendor: nextbricks					
Product: bricksore					
Affected Version(s): * Up to (including) 1.4.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Aug-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nextbricks Brickscore allows Stored XSS.This issue affects Brickscore: from n/a through 1.4.2.5.	N/A	A-NEX-BRIC-030924/292

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43950		
Vendor: nicmx					
Product: fort-validator					
Affected Version(s): * Up to (excluding) 1.6.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Aug-2024	9.8	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a resource certificate containing a Key Usage extension composed of more than two bytes of data. Fort writes this string into a 2-byte buffer without properly sanitizing its length, leading to a buffer overflow. **CVE ID: CVE-2024-45237**	https://nicmx.github.io/FORT-validator/CVE.html	A-NIC-FORT-030924/293
N/A	24-Aug-2024	7.5	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) an ROA or a Manifest containing a signedAttrs encoded in non-	N/A	A-NIC-FORT-030924/294

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			canonical form. This bypasses Fort's BER decoder, reaching a point in the code that panics when faced with data not encoded in DER. Because Fort is an RPKI Relying Party, a panic can lead to Route Origin Validation unavailability, which can lead to compromised routing. **CVE ID: CVE-2024-45234**		
N/A	24-Aug-2024	7.5	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) a signed object containing an empty signedAttributes field. Fort accesses the set's elements without sanitizing it first. Because Fort is an RPKI Relying Party, a crash can lead to Route Origin Validation unavailability, which can lead to	https://nicmx.github.io/FORT-validator/CVE.html	A-NIC-FORT-030924/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromised routing. **CVE ID: CVE-2024-45236**		
NULL Pointer Dereference	24-Aug-2024	7.5	An issue was discovered in Fort before 1.6.3. A malicious RPKI repository that descends from a (trusted) Trust Anchor can serve (via rsync or RRDP) an ROA or a Manifest containing a null eContent field. Fort dereferences the pointer without sanitizing it first. Because Fort is an RPKI Relying Party, a crash can lead to Route Origin Validation unavailability, which can lead to compromised routing. **CVE ID: CVE-2024-45239**	N/A	A-NIC-FORT-030924/296
Vendor: okfn					
Product: ckan					
Affected Version(s): * Up to (excluding) 2.10.5					
Server-Side Request Forgery (SSRF)	21-Aug-2024	6.5	CKAN is an open-source data management system for powering data hubs and data portals. There are a number of CKAN plugins,	https://github.com/ckan/ckan/security/advisories/GHSA-g9ph-j5vj-f8wm	A-OKF-CKAN-030924/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	including XLoader, DataPusher, Resource proxy and ckanext-archiver, that work by downloading the contents of local or remote files in order to perform some actions with their contents (e.g. pushing to the DataStore, streaming contents or saving a local copy). All of them use the resource URL, and there are currently no checks to limit what URLs can be requested. This means that a malicious (or unaware) user can create a resource with a URL pointing to a place where they should not have access in order for one of the previous tools to retrieve it (known as a Server Side Request Forgery). Users wanting to protect against these kinds of attacks can use one or a combination of the following approaches: (1) Use a separate HTTP proxy like Squid that can be		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to allow / disallow IPs, domains etc as needed, and make CKAN extensions aware of this setting via the ckan.download_proxy config option. (2) Implement custom firewall rules to prevent access to restricted resources. (3) Use custom validators on the resource url field to block/allow certain domains or IPs. All latest versions of the plugins listed above support the ckan.download_proxy settings. Support for this setting in the Resource Proxy plugin was included in CKAN 2.10.5 and 2.11.0. **CVE ID: CVE-2024-43371**		
Affected Version(s): From (including) 2.0 Up to (excluding) 2.10.5					
Generation of Error Message Containing Sensitive Information	21-Aug-2024	5.3	CKAN is an open-source data management system for powering data hubs and data portals. If there were connection issues with the Solr server, the internal Solr URL	https://github.com/ckan/ckan/commit/f6b032cd7082d784938165bbd113557639002ca7, https://github.com/ckan/ckan/security/advisories/GHSA-2rqw-cfhc-35fh	A-OKF-CKAN-030924/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(potentially including credentials) could be leaked to package_search calls as part of the returned error message. This has been patched in CKAN 2.10.5 and 2.11.0. **CVE ID: CVE-2024-41674**		
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.10.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-2024	6.1	CKAN is an open-source data management system for powering data hubs and data portals. The Datatables view plugin did not properly escape record data coming from the DataStore, leading to a potential XSS vector. Sites running CKAN >= 2.7.0 with the datatables_view plugin activated. This is a plugin included in CKAN core, that not activated by default but it is widely used to preview tabular data. This vulnerability has been fixed in CKAN 2.10.5 and 2.11.0.	https://github.com/ckan/ckan/commit/9e89ce8220ab1445e0bd85a67994a51d9d3d2688, https://github.com/ckan/ckan/commit/d7dfe8c427b1c63c75d788a609f3b7d7620a25a1, https://github.com/ckan/ckan/security/advisories/GHSA-r3jc-vhf4-6v32	A-OKF-CKAN-030924/299

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41675		
Vendor: ollama					
Product: ollama					
Affected Version(s): * Up to (excluding) 0.1.47					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Aug-2024	7.5	extractFromZipFile in model.go in Ollama before 0.1.47 can extract members of a ZIP archive outside of the parent directory. **CVE ID: CVE-2024-45436**	https://github.com/ollama/ollama/compare/v0.1.46...v0.1.47, https://github.com/ollama/ollama/pull/5314	A-OLL-OLLA-030924/300
Vendor: online_railway_reservation_system_project					
Product: online_railway_reservation_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	18-Aug-2024	7.2	A vulnerability was found in CodeAstro Online Railway Reservation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/emp-profile-avatar.php of the component Profile Photo Update Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the	N/A	A-ONL-ONLI-030924/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. **CVE ID: CVE-2024-7910**		
N/A	18-Aug-2024	5.3	A vulnerability was found in CodeAstro Online Railway Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/assets/. The manipulation leads to exposure of information through directory listing. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7912**	N/A	A-ONL-ONLI-030924/302
Vendor: opensecurity					
Product: mobile_security_framework					
Affected Version(s): * Up to (excluding) 4.0.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Aug-2024	9.8	Mobile Security Framework (MobSF) is a pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. Before	https://github.com/MobSF/Mobile-Security-Framework-MobSF/commit/cc625fe8430f3437a473e82aa2966d100a4dc883, https://github.com/MobSF/Mo	A-OPE-MOBI-030924/303

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.0.7, there is a flaw in the Static Libraries analysis section. Specifically, during the extraction of .a extension files, the measure intended to prevent Zip Slip attacks is improperly implemented. Since the implemented measure can be bypassed, the vulnerability allows an attacker to extract files to any desired location within the server running MobSF. This vulnerability is fixed in 4.0.7. **CVE ID: CVE-2024-43399**	bile-Security-Framework-MobSF/security/advisories/GHSA-4hh3-vj32-gr6j	
Vendor: oretnom23					
Product: clinic_patient_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Aug-2024	8.8	A vulnerability has been found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /pms/ajax/get_packings.php. The manipulation of the	N/A	A-ORE-CLIN-030924/304

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument medicine_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7930**		
Product: music_gallery_site					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8221**	N/A	A-ORE-MUSI-030924/305
Improper Neutralization of Special	27-Aug-2024	9.8	A vulnerability classified as critical has been found in SourceCodester	N/A	A-ORE-MUSI-030924/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Music Gallery Site 1.0. This affects an unknown part of the file /admin/?page=musics/manage_music. 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. **CVE ID: CVE-2024-8222**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in SourceCodester Music Gallery Site 1.0. This vulnerability affects unknown code of the file /classes/Master.php?f=delete_category. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8223**	N/A	A-ORE-MUSI-030924/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: online_computer_and_laptop_store					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Aug-2024	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file /php-ocls/classes/Master.php?f=pay_order. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8083**	N/A	A-ORE-ONLI-030924/308
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Aug-2024	4.8	A vulnerability, which was classified as problematic, was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file /php-ocls/classes/SystemSettings.php?f=update_settings of the component	N/A	A-ORE-ONLI-030924/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Setting Handler. The manipulation of the argument System 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. **CVE ID: CVE-2024-8084**		
Product: simple_forum_website					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-2024	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Forum Website 1.0. This affects an unknown part of the file /registration.php of the component Signup Page. The manipulation of the argument username 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.	N/A	A-ORE-SIMP-030924/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7929		
Product: simple_online_bidding_system					
Affected Version(s): 1.0					
Externally Controlled Reference to a Resource in Another Sphere	18-Aug-2024	9.8	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as critical. This affects an unknown part of the file /simple-online-bidding-system/bidding/index.php. The manipulation of the argument page leads to file inclusion. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7911**	N/A	A-ORE-SIMP-030924/311
Product: yoga_class_registration_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Aug-2024	5.4	A vulnerability classified as problematic has been found in SourceCodester Yoga Class Registration System 1.0. Affected is an unknown function	N/A	A-ORE-YOGA-030924/312

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the file /php-ycrs/classes/SystemSettings.php. The manipulation of the argument address 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. **CVE ID: CVE-2024-7914**		
Vendor: pagebuilderaddons					
Product: web_and_woocommerce_addons_for_wpbakery_builder					
Affected Version(s): * Up to (including) 1.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Aug-2024	4.8	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Page Builder Addons Web and WooCommerce Addons for WPBakery Builder allows Stored XSS.This issue affects Web and WooCommerce Addons for WPBakery Builder: from n/a through 1.4.6. **CVE ID: CVE-2024-43960**	N/A	A-PAG-WEB_-030924/313

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: pharmacy_management_system_project					
Product: pharmacy_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in code-projects Pharmacy Management System 1.0. Affected is the function editManager of the file /index.php?action=editManager of the component Parameter Handler. The manipulation of the argument id as part of String leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. **CVE ID: CVE-2024-8138**	N/A	A-PHA-PHAR-030924/314
Vendor: Pligg					
Product: pligg_cms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0.2					
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/submit_page.php. **CVE ID: CVE-2024-42608**	N/A	A-PLI-PLIG-030924/315
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_backup.php?dobackup=clearall **CVE ID: CVE-2024-42603**	N/A	A-PLI-PLIG-030924/316
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_group.php?mode=delete&group_id=3 **CVE ID: CVE-2024-42604**	N/A	A-PLI-PLIG-030924/317
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/edit_page.php?link_id=1	N/A	A-PLI-PLIG-030924/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42605		
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_log.php?clear=1 **CVE ID: CVE-2024-42606**	N/A	A-PLI-PLIG-030924/319
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_backup.php?dobackup=database **CVE ID: CVE-2024-42607**	N/A	A-PLI-PLIG-030924/320
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_backup.php?dobackup=avatars **CVE ID: CVE-2024-42609**	N/A	A-PLI-PLIG-030924/321
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_bac	N/A	A-PLI-PLIG-030924/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kup.php?dobackup=files **CVE ID: CVE-2024-42610**		
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) via admin/admin_page.php?link_id=1&mode=delete **CVE ID: CVE-2024-42611**	N/A	A-PLI-PLIG-030924/323
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_widgets.php?action=install&widget=akismet **CVE ID: CVE-2024-42613**	N/A	A-PLI-PLIG-030924/324
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_widgets.php?action=remove&widget=Statistics **CVE ID: CVE-2024-42616**	N/A	A-PLI-PLIG-030924/325
Cross-Site Request	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site	N/A	A-PLI-PLIG-030924/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Request Forgery (CSRF) vulnerability via /admin/admin_config.php?action=save&var_id=32 **CVE ID: CVE-2024-42617**		
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /module.php?module=karma **CVE ID: CVE-2024-42618**	N/A	A-PLI-PLIG-030924/327
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_editor.php **CVE ID: CVE-2024-42621**	N/A	A-PLI-PLIG-030924/328
Vendor: projectcapsule					
Product: capsule					
Affected Version(s): * Up to (including) 0.7.0					
Incorrect Authorization	20-Aug-2024	8.8	Capsule is a multi-tenancy and policy-based framework for Kubernetes. In Capsule v0.7.0 and earlier, the tenant-owner can patch any arbitrary namespace that has not been taken over	https://github.com/projectcapsule/capsule/commit/d620b0457ddec01616b8eab8512a10611611f584	A-PRO-CAPS-030924/329

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a tenant (i.e., namespaces without the ownerReference field), thereby gaining control of that namespace. **CVE ID: CVE-2024-39690**		
Vendor: project_expense_monitoring_system_project					
Product: project_expense_monitoring_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Aug-2024	9.8	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been classified as critical. Affected is an unknown function of the file login1.php of the component Backend Login. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7933**	N/A	A-PRO-PROJ-030924/330
Improper Neutralization of Special	19-Aug-2024	9.8	A vulnerability was found in itsourcecode Project Expense	N/A	A-PRO-PROJ-030924/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Monitoring System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file execute.php. The manipulation of the argument code leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7934**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Aug-2024	9.8	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file print.php. The manipulation of the argument map_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-PRO-PROJ-030924/332

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7935		
Vendor: PTC					
Product: thingworx					
Affected Version(s): 9.5.0					
Authorization Bypass Through User-Controlled Key	27-Aug-2024	6.5	An Insecure Direct Object Reference (IDOR) in PTC ThingWorx v9.5.0 allows attackers to view sensitive information, including PII, regardless of access level. **CVE ID: CVE-2024-40395**	N/A	A-PTC-THIN-030924/333
Vendor: public_knowledge_project					
Product: open_journal_systems					
Affected Version(s): * Up to (including) 3.4.0-6					
URL Redirection to Untrusted Site ('Open Redirect')	17-Aug-2024	6.1	A vulnerability was found in pkp ojs up to 3.4.0-6 and classified as problematic. Affected by this issue is some unknown functionality of the file /login/signOut. The manipulation of the argument source with the input .example.com leads to open redirect. The attack may be launched remotely. The exploit has been disclosed to the public and may be	N/A	A-PUB-OPEN-030924/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7902**		
Vendor: Python					
Product: python					
Affected Version(s): * Up to (including) 3.12.5					
N/A	19-Aug-2024	7.5	There is a LOW severity vulnerability affecting CPython, specifically the 'http.cookies' standard library module. When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value.	https://github.com/python/cpython/issues/123067, https://github.com/python/cpython/pull/123075	A-PYT-PYTH-030924/335

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7592		
Affected Version(s): 3.13.0					
N/A	19-Aug-2024	7.5	There is a LOW severity vulnerability affecting CPython, specifically the 'http.cookies' standard library module. When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value. **CVE ID: CVE-2024-7592**	https://github.com/python/cpython/issues/123067, https://github.com/python/cpython/pull/123075	A-PYT-PYTH-030924/336
Vendor: rakuten					
Product: ichiba					
Affected Version(s): * Up to (including) 11.7.0					
Missing Authorization	29-Aug-2024	6.1	'Rakuten Ichiba App' for Android 12.4.0 and earlier and 'Rakuten Ichiba App' for iOS 11.7.0	N/A	A-RAK-ICHI-030924/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier are vulnerable to improper authorization in handler for custom URL scheme. An arbitrary site may be displayed on the WebView of the product via Intent from another application installed on the user's device. As a result, the user may be redirected to an unauthorized site, and the user may become a victim of a phishing attack. **CVE ID: CVE-2024-41918**		
Affected Version(s): * Up to (including) 12.4.0					
Missing Authorization	29-Aug-2024	6.1	'Rakuten Ichiba App' for Android 12.4.0 and earlier and 'Rakuten Ichiba App' for iOS 11.7.0 and earlier are vulnerable to improper authorization in handler for custom URL scheme. An arbitrary site may be displayed on the WebView of the product via Intent from another application installed on the user's device. As a result, the user may	N/A	A-RAK-ICHI-030924/338

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be redirected to an unauthorized site, and the user may become a victim of a phishing attack. **CVE ID: CVE-2024-41918**		
Vendor: Redhat					
Product: build_of_apache_camel_-_hawtio					
Affected Version(s): -					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-BUIL-030924/339

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: build_of_apache_camel_for_spring_boot					
Affected Version(s): -					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-BUIL-030924/340

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: build_of_keycloak					
Affected Version(s): -					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-BUIL-030924/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: data_grid					
Affected Version(s): 8.0.0					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-DATA-030924/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: integration_camel_k					
Affected Version(s): -					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-INTE-030924/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: jboss_enterprise_application_platform					
Affected Version(s): 8.0.0					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-JBOS-030924/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Affected Version(s): 7.0.0					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-JBOS-030924/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: jboss_fuse					
Affected Version(s): 7.0.0					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-JBOS-030924/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: openstack_platform					
Affected Version(s): 16.1					
Improper Certificate Validation	21-Aug-2024	8.1	A flaw was found in the Red Hat OpenStack Platform (RHOSP) director. This vulnerability allows an attacker to deploy potentially	https://access.redhat.com/security/cve/CVE-2024-8007, https://bugzilla.redhat.com/show_bug.cgi?id=2305975	A-RED-OPEN-030924/347

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromised container images via disabling TLS certificate verification for registry mirrors, which could enable a man-in-the-middle (MITM) attack. **CVE ID: CVE-2024-8007**		
Affected Version(s): 16.2					
Improper Certificate Validation	21-Aug-2024	8.1	A flaw was found in the Red Hat OpenStack Platform (RHOSP) director. This vulnerability allows an attacker to deploy potentially compromised container images via disabling TLS certificate verification for registry mirrors, which could enable a man-in-the-middle (MITM) attack. **CVE ID: CVE-2024-8007**	https://access.redhat.com/security/cve/CVE-2024-8007, https://bugzilla.redhat.com/show_bug.cgi?id=2305975	A-RED-OPEN-030924/348
Affected Version(s): 17.1					
Improper Certificate Validation	21-Aug-2024	8.1	A flaw was found in the Red Hat OpenStack Platform (RHOSP) director. This vulnerability allows an attacker	https://access.redhat.com/security/cve/CVE-2024-8007, https://bugzilla.redhat.com/sh	A-RED-OPEN-030924/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to deploy potentially compromised container images via disabling TLS certificate verification for registry mirrors, which could enable a man-in-the-middle (MITM) attack. **CVE ID: CVE-2024-8007**	ow_bug.cgi?id=2305975	
Product: process_automation					
Affected Version(s): 7.0					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-PROC-030924/350

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Product: single_sign-on					
Affected Version(s): 7.0					
N/A	21-Aug-2024	7.5	A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between	https://access.redhat.com/security/cve/CVE-2024-7885, https://bugzilla.redhat.com/show_bug.cgi?id=2305290	A-RED-SING-030924/351

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. **CVE ID: CVE-2024-7885**		
Vendor: rems					
Product: account_manager_app					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	5.4	A vulnerability classified as problematic was found in SourceCodester Accounts Manager App 1.0. This vulnerability affects unknown code of the file update-account.php of the component Update Account Page. The manipulation of the argument Account Name/Username/Password/Link leads to cross site	N/A	A-REM-ACCO-030924/352

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7948**		
Product: daily_calories_monitoring_tool					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-2024	5.4	A vulnerability was found in SourceCodester Daily Calories Monitoring Tool 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/add-calorie.php. The manipulation of the argument calorie_date/calorie_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. **CVE ID: CVE-2024-8141**	N/A	A-REM-DAIL-030924/353
Improper Neutralization of Input During Web Page	25-Aug-2024	5.4	A vulnerability was found in SourceCodester Daily Calories Monitoring Tool	N/A	A-REM-DAIL-030924/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /endpoint/delete-calorie.php. The manipulation of the argument calorie leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8142**		
Product: interactive_map_with_marker					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-2024	5.4	A vulnerability was found in SourceCodester Interactive Map with Marker 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/delete-mark.php. The manipulation of the argument mark leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the	N/A	A-REM-INTE-030924/355

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. **CVE ID: CVE-2024-8151**		
Product: qr_code_attendance_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Aug-2024	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester QR Code Attendance System 1.0. This issue affects some unknown processing of the file /endpoint/delete-student.php. The manipulation of the argument student/attendance leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8172**	N/A	A-REM-QR_C-030924/356
Product: qr_code_bookmark_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	25-Aug-2024	5.4	A vulnerability was found in SourceCodester QR Code Bookmark System 1.0. It has been declared as	N/A	A-REM-QR_C-030924/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			problematic. This vulnerability affects unknown code of the file /endpoint/add-bookmark.php of the component Parameter Handler. The manipulation of the argument name/url leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8152**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-2024	5.4	A vulnerability was found in SourceCodester QR Code Bookmark System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /endpoint/delete-bookmark.php. The manipulation of the argument bookmark leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-REM-QR_C-030924/358

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8153		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-2024	5.4	A vulnerability classified as problematic has been found in SourceCodester QR Code Bookmark System 1.0. Affected is an unknown function of the file /endpoint/update-bookmark.php of the component Parameter Handler. The manipulation of the argument tbl_bookmark_id/name/url 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. **CVE ID: CVE-2024-8154**	N/A	A-REM-QR_C-030924/359
Product: task_progress_tracker					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Aug-2024	5.4	A vulnerability was found in SourceCodester Task Progress Tracker 1.0 and classified as problematic. Affected by this issue is some unknown	N/A	A-REM-TASK-030924/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality of the file update-task.php. The manipulation of the argument task_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-8140**		
Product: zipped_folder_manager_app					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	26-Aug-2024	9.8	A vulnerability classified as problematic has been found in SourceCodester Zipped Folder Manager App 1.0. This affects an unknown part of the file /endpoint/add-folder.php. The manipulation of the argument folder leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	N/A	A-REM-ZIPP-030924/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8170		
Vendor: retool					
Product: retool					
Affected Version(s): From (including) 3.18.1 Up to (including) 3.40.0					
Insertion of Sensitive Information into Log File	22-Aug-2024	6.5	Retool (self-hosted enterprise) through 3.40.0 inserts resource authentication credentials into sent data. Credentials for users with "Use" permissions can be discovered (by an authenticated attacker) via the /api/resources endpoint. The earliest affected version is 3.18.1. **CVE ID: CVE-2024-42056**	https://docs.retool.com/disclosures/cve-2024-42056	A-RET-RETO-030924/362
Vendor: rubrik					
Product: cloud_data_management					
Affected Version(s): * Up to (excluding) 8.1.3					
N/A	27-Aug-2024	8.8	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code. **CVE ID: CVE-2024-36068**	https://www.rubrik.com/advisories/rbk-20240619-v0044	A-RUB-CLOU-030924/363

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 8.1.3					
N/A	27-Aug-2024	8.8	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code. **CVE ID: CVE-2024-36068**	https://www.rubrik.com/advisories/rbk-20240619-v0044	A-RUB-CLOU-030924/364
Affected Version(s): 9.0.3					
N/A	27-Aug-2024	8.8	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code. **CVE ID: CVE-2024-36068**	https://www.rubrik.com/advisories/rbk-20240619-v0044	A-RUB-CLOU-030924/365
Affected Version(s): 9.1.2					
N/A	27-Aug-2024	8.8	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code.	https://www.rubrik.com/advisories/rbk-20240619-v0044	A-RUB-CLOU-030924/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-36068		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.3					
N/A	27-Aug-2024	8.8	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code. **CVE ID: CVE-2024-36068**	https://www.rubrik.com/advisories/rbk-20240619-v0044	A-RUB-CLOU-030924/367
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.2					
N/A	27-Aug-2024	8.8	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code. **CVE ID: CVE-2024-36068**	https://www.rubrik.com/advisories/rbk-20240619-v0044	A-RUB-CLOU-030924/368
Vendor: rust-bitcoin					
Product: miniscript					
Affected Version(s): * Up to (excluding) 12.2.0					
Out-of-bounds Write	19-Aug-2024	7.5	The Miniscript (aka rust-miniscript) library before 12.2.0 for Rust allows stack consumption because it does not	https://github.com/rust-bitcoin/rust-miniscript/compare/11.2.0...12.2.0, https://github.c	A-RUS-MINI-030924/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly track tree depth. **CVE ID: CVE-2024-44073**	om/rust-bitcoin/rust-miniscript/pull/704, https://github.com/rust-bitcoin/rust-miniscript/pull/712	
Vendor: scada-lts					
Product: scada-lts					
Affected Version(s): 2.7.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-2024	5.4	A vulnerability has been found in Scada-LTS 2.7.8 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /Scada-LTS/app.shtm#/alarms/Scada of the component Message Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: A fix is planned for the upcoming release at the end of September 2024. **CVE ID: CVE-2024-7901**	N/A	A-SCA-SCAD-030924/370
Vendor: Servision					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ivg_webmax					
Affected Version(s): 1.0.57					
Improper Authentication	20-Aug-2024	9.8	Servision - CWE-287: Improper Authentication **CVE ID: CVE-2024-42336**	N/A	A-SER-IVG_-030924/371
Vendor: siamonhasan					
Product: warehouse_inventory_system					
Affected Version(s): 2.0					
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	A Cross-Site Request Forgery (CSRF) in the component add_product.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges. **CVE ID: CVE-2024-42577**	N/A	A-SIA-WARE-030924/372
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	A Cross-Site Request Forgery (CSRF) in the component add_group.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges. **CVE ID: CVE-2024-42579**	N/A	A-SIA-WARE-030924/373
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	A Cross-Site Request Forgery (CSRF) in the component edit_group.php of Warehouse	N/A	A-SIA-WARE-030924/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Inventory System v2.0 allows attackers to escalate privileges. **CVE ID: CVE-2024-42580**		
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	A Cross-Site Request Forgery (CSRF) in the component delete_group.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges. **CVE ID: CVE-2024-42581**	N/A	A-SIA-WARE-030924/375
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	A Cross-Site Request Forgery (CSRF) in the component delete_categorie.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges. **CVE ID: CVE-2024-42582**	N/A	A-SIA-WARE-030924/376
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	A Cross-Site Request Forgery (CSRF) in the component delete_user.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.	N/A	A-SIA-WARE-030924/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42583		
Cross-Site Request Forgery (CSRF)	20-Aug-2024	8.8	A Cross-Site Request Forgery (CSRF) in the component delete_product.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges. **CVE ID: CVE-2024-42584**	N/A	A-SIA-WARE-030924/378
Vendor: skyss					
Product: arfa-cms					
Affected Version(s): * Up to (excluding) 5.1.3124					
Cross-Site Request Forgery (CSRF)	27-Aug-2024	8.8	A cross-site request forgery (CSRF) vulnerability in the admin panel in SkySystem Arfa-CMS before 5.1.3124 allows remote attackers to add a new administrator, leading to escalation of privileges. **CVE ID: CVE-2024-45264**	N/A	A-SKY-ARFA-030924/379
Vendor: smashballoon					
Product: reviews_feed					
Affected Version(s): * Up to (excluding) 1.2.0					
Missing Authorization	27-Aug-2024	4.3	The Reviews Feed – Add Testimonials and Customer Reviews From Google Reviews,	https://plugins.trac.wordpress.org/changeset/3125315/, https://www.w	A-SMA-REVI-030924/380

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Yelp, TripAdvisor, and More plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_api_key' function in all versions up to, and including, 1.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update API Key options. **CVE ID: CVE-2024-8199**	ordfence.com/threat-intel/vulnerabilities/id/dc3e89e5-2e7e-497e-b340-b787ebdf3711?source=cve	
Cross-Site Request Forgery (CSRF)	27-Aug-2024	4.3	The Reviews Feed – Add Testimonials and Customer Reviews From Google Reviews, Yelp, TripAdvisor, and More plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the 'update_api_key' function. This makes it possible	https://plugins.trac.wordpress.org/changeset/3125315/, https://www.wordfence.com/threat-intel/vulnerabilities/id/5d9e20f7-813c-4691-bce4-d0ff4774ae48?source=cve	A-SMA-REVI-030924/381

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for unauthenticated attackers to update an API key via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-8200**		
Vendor: softlabbd					
Product: radio_player					
Affected Version(s): * Up to (excluding) 2.0.74					
Missing Authorization	17-Aug-2024	5.3	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_player function in versions up to, and including, 2.0.73. This makes it possible for unauthenticated attackers to delete player instances. **CVE ID: CVE-2023-4024**	https://plugins.trac.wordpress.org/changeset/2942906/radio-player/trunk/includes/class-ajax.php, https://plugins.trac.wordpress.org/changeset/3048105	A-SOF-RADI-030924/382
Missing Authorization	17-Aug-2024	5.3	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of	https://plugins.trac.wordpress.org/changeset/2942906/radio-player/trunk/includes/class-	A-SOF-RADI-030924/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data due to a missing capability check on the update_player function in versions up to, and including, 2.0.73. This makes it possible for unauthenticated attackers to update player instances. **CVE ID: CVE-2023-4025**	ajax.php, https://plugins.trac.wordpress.org/changeset/3048105	
Vendor: sportsnet					
Product: sportsnet					
Affected Version(s): 4.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/conexiones/ax/openTracExt/, parameter categoria;. **CVE ID: CVE-2024-29723**	N/A	A-SPO-SPOR-030924/384
Improper Neutralization of Special	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version	N/A	A-SPO-SPOR-030924/385

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/ax/registerSp/, parameter idDesafio. **CVE ID: CVE-2024-29724**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/sort_bloques/, parameter list. **CVE ID: CVE-2024-29725**	N/A	A-SPO-SPOR-030924/386
Improper Neutralization of Special Elements used in an SQL Command	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve,	N/A	A-SPO-SPOR-030924/387

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/setAsRead/, parameter id. **CVE ID: CVE-2024-29726**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/sendParticipationRemember/ , parameter send. **CVE ID: CVE-2024-29727**	N/A	A-SPO-SPOR-030924/388
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially	N/A	A-SPO-SPOR-030924/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/inscribeUsuario/ , parameter idDesafio. **CVE ID: CVE-2024-29728**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/generateShortURL/, parameter url. **CVE ID: CVE-2024-29729**	N/A	A-SPO-SPOR-030924/390
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio	N/A	A-SPO-SPOR-030924/391

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.com/app/ax/consejoRandom/ , parameter idCat;. **CVE ID: CVE-2024-29730**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Aug-2024	9.8	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/checkBlindFields/ , parameters idChallenge and idEmpresa. **CVE ID: CVE-2024-29731**	N/A	A-SPO-SPOR-030924/392
Vendor: squirrelly					
Product: squirrelly					
Affected Version(s): 9.0.0					
Improper Control of Generation of Code ('Code Injection')	21-Aug-2024	9.8	squirrellyjs squirrelly v9.0.0 and fixed in v.9.0.1 was discovered to contain a code injection vulnerability via the component options.varName. **CVE ID: CVE-2024-40453**	https://github.com/squirrellyjs/squirrelly/pull/262	A-SQU-SQUI-030924/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: sunmochina					
Product: enterprise_management_system					
Affected Version(s): From (including) 5.0 Up to (including) 18.8					
N/A	28-Aug-2024	7.5	Incorrect access control in the component /servlet/SnoopServlet of Shenzhou News Union Enterprise Management System v5.0 through v18.8 allows attackers to access sensitive information regarding the server. **CVE ID: CVE-2024-44760**	N/A	A-SUN-ENTE-030924/394
Vendor: tamparongj_03					
Product: online_graduate_tracer_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Aug-2024	8.8	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. This issue affects some unknown processing of the file /tracking/admin/view_csprofile.php. The manipulation of the argument id leads to sql injection. The attack may be	N/A	A-TAM-ONLI-030924/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7931**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Aug-2024	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Graduate Tracer System up to 1.0. Affected is an unknown function of the file /tracking/admin/fetch_genderit.php. The manipulation of the argument request leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7949**	N/A	A-TAM-ONLI-030924/396
Vendor: themeum					
Product: droip					
Affected Version(s): * Up to (including) 1.1.1					
Improper Limitation of a Pathname to a Restricted Directory	29-Aug-2024	7.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in	N/A	A-THE-DROI-030924/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Themeum Droip allows File Manipulation.This issue affects Droip: from n/a through 1.1.1. **CVE ID: CVE-2024-43955**		
Incorrect Authorization	29-Aug-2024	6.3	Incorrect Authorization vulnerability in Themeum Droip allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Droip: from n/a through 1.1.1. **CVE ID: CVE-2024-43954**	N/A	A-THE-DROI-030924/398
Vendor: tpmecms					
Product: tpmecms					
Affected Version(s): 1.3.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Aug-2024	4.8	A vulnerability, which was classified as problematic, was found in xiaohe4966 TpMeCMS 1.3.3.2. Affected is an unknown function of the file /h.php/general/config?ref=addtabs of the component Basic Configuration Handler. The manipulation of the argument Site Name/Beian/Conta	N/A	A-TPM-TPME-030924/399

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ct address/copyright /technical support 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. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7900**		
Vendor: trufflesecurity					
Product: trufflehog					
Affected Version(s): * Up to (excluding) 3.81.9					
Server-Side Request Forgery (SSRF)	19-Aug-2024	3.1	TruffleHog is a secrets scanning tool. Prior to v3.81.9, this vulnerability allows a malicious actor to craft data in a way that, when scanned by specific detectors, could trigger the detector to make an unauthorized request to an endpoint chosen by the attacker. For an exploit to be effective, the target endpoint must be	https://github.com/trufflesecurity/trufflehog/commit/fe5624c709233551288 68cffd647b6e2cfe11443, https://github.com/trufflesecurity/trufflehog/security/advisories/GHSA-3r74-v83p-f4f4	A-TRU-TRUF-030924/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated GET endpoint that produces side effects. The victim must scan the maliciously crafted data and have such an endpoint targeted for the exploit to succeed. The vulnerability has been resolved in TruffleHog v3.81.9 and later versions. **CVE ID: CVE-2024-43379**		
Vendor: typecho					
Product: typecho					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	9	A stored cross-site scripting (XSS) vulnerability in Typecho v1.3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID: CVE-2024-35540**	N/A	A-TYP-TYPE-030924/401
Affected Version(s): 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	9	A stored cross-site scripting (XSS) vulnerability in Typecho v1.3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	N/A	A-TYP-TYPE-030924/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-35540		
Vendor: Umbraco					
Product: umbraco_cms					
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.1.2					
Generation of Error Message Containing Sensitive Information	20-Aug-2024	5.3	Umbraco is an ASP.NET CMS. Some endpoints in the Management API can return stack trace information, even when Umbraco is not in debug mode. This vulnerability is fixed in 14.1.2. **CVE ID: CVE-2024-43376**	https://github.com/umbraco/Umbraco-CMS/commit/b76070c794925932cb159ef50b851db6e966a004, https://github.com/umbraco/Umbraco-CMS/security/advisories/GHSA-77gj-crhp-3gvx	A-UMB-UMBR-030924/403
N/A	20-Aug-2024	4.3	Umbraco CMS is an ASP.NET CMS. An authenticated user can access a few unintended endpoints. This issue is fixed in 14.1.2. **CVE ID: CVE-2024-43377**	https://github.com/umbraco/Umbraco-CMS/commit/72bef8861d94a39d5cc9530a04c4797b91fcbecf, https://github.com/umbraco/Umbraco-CMS/security/advisories/GHSA-hrww-x3fq-xcvh	A-UMB-UMBR-030924/404
Vendor: upkeeper					
Product: upkeeper_manager					
Affected Version(s): * Up to (excluding) 5.1.10					
Improper Authentication	16-Aug-2024	9.8	Improper Authentication vulnerability in upKeeper Solutions product upKeeper	https://support.upkeeper.se/hc/en-us/articles/15432045399452-	A-UPK-UPKE-030924/405

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager allows Authentication Bypass.This issue affects upKeeper Manager: through 5.1.9. **CVE ID: CVE-2024-42462**	CVE-2024-42462-Bypass-multifactor-authentication	
Improper Restriction of Excessive Authentication Attempts	16-Aug-2024	9.8	Improper Restriction of Excessive Authentication Attempts vulnerability in upKeeper Solutions product upKeeper Manager allows Authentication Abuse.This issue affects upKeeper Manager: through 5.1.9. **CVE ID: CVE-2024-42466**	https://support.upkeeper.se/hc/en-us/articles/15432408367260-CVE-2024-42466-Lack-of-resources-and-rate-limiting-login	A-UPK-UPKE-030924/406
Authorization Bypass Through User-Controlled Key	16-Aug-2024	6.5	Authorization Bypass Through User-Controlled Key vulnerability in upKeeper Solutions product upKeeper Manager allows Utilizing REST's Trust in the System Resource to Obtain Sensitive Data.This issue affects upKeeper Manager: through 5.1.9. **CVE ID: CVE-2024-42463**	https://support.upkeeper.se/hc/en-us/articles/15432241822620-CVE-2024-42463-Leak-of-organizations-messages	A-UPK-UPKE-030924/407
Authorization Bypass	16-Aug-2024	6.5	Authorization Bypass Through	https://support.upkeeper.se/hc	A-UPK-UPKE-030924/408

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Through User-Controlled Key			User-Controlled Key vulnerability in upKeeper Solutions product upKeeper Manager allows Utilizing REST's Trust in the System Resource to Obtain Sensitive Data.This issue affects upKeeper Manager: through 5.1.9. **CVE ID: CVE-2024-42464**	/en-us/articles/15432275702044-CVE-2024-42464-Leak-of-user-Information	
Affected Version(s): * Up to (including) 5.1.10					
Improper Restriction of Excessive Authentication Attempts	16-Aug-2024	9.8	Improper Restriction of Excessive Authentication Attempts vulnerability in upKeeper Solutions product upKeeper Manager allows Authentication Abuse.This issue affects upKeeper Manager: through 5.1.9. **CVE ID: CVE-2024-42465**	https://support.upkeeper.se/hc/en-us/articles/15432332385564-CVE-2024-42465-Lack-of-resources-and-rate-limiting-two-factor-authentication	A-UPK-UPKE-030924/409
Vendor: versa-networks					
Product: versa_director					
Affected Version(s): 21.2.2					
Unrestricted Upload of File with Dangerous Type	22-Aug-2024	7.2	The Versa Director GUI provides an option to customize the look and feel of the user interface. This option is only available for a user	https://versa-networks.com/blog/versa-security-bulletin-update-on-cve-2024-39717-versa-	A-VER-VERS-030924/410

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logged with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin. (Tenant level users do not have this privilege). The "Change Favicon" (Favorite Icon) option can be mis-used to upload a malicious file ending with .png extension to masquerade as image file. This is possible only after a user with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin has successfully authenticated and logged in. **CVE ID: CVE-2024-39717**	director-dangerous-file-type-upload-vulnerability/	
Affected Version(s): 21.2.3					
Unrestricted Upload of File with Dangerous Type	22-Aug-2024	7.2	The Versa Director GUI provides an option to customize the look and feel of the user interface. This option is only available for a user logged with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin. (Tenant	https://versa-networks.com/blog/versa-security-bulletin-update-on-cve-2024-39717-versa-director-dangerous-file-type-upload-vulnerability/	A-VER-VERS-030924/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level users do not have this privilege). The "Change Favicon" (Favorite Icon) option can be mis-used to upload a malicious file ending with .png extension to masquerade as image file. This is possible only after a user with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin has successfully authenticated and logged in. **CVE ID: CVE-2024-39717**		
Affected Version(s): 22.1.1					
Unrestricted Upload of File with Dangerous Type	22-Aug-2024	7.2	The Versa Director GUI provides an option to customize the look and feel of the user interface. This option is only available for a user logged with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin. (Tenant level users do not have this privilege). The "Change Favicon" (Favorite Icon) option can be mis-used to upload	https://versa-networks.com/blog/versa-security-bulletin-update-on-cve-2024-39717-versa-director-dangerous-file-type-upload-vulnerability/	A-VER-VERS-030924/412

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious file ending with .png extension to masquerade as image file. This is possible only after a user with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin has successfully authenticated and logged in. **CVE ID: CVE-2024-39717**		
Affected Version(s): 22.1.2					
Unrestricted Upload of File with Dangerous Type	22-Aug-2024	7.2	The Versa Director GUI provides an option to customize the look and feel of the user interface. This option is only available for a user logged with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin. (Tenant level users do not have this privilege). The "Change Favicon" (Favorite Icon) option can be mis-used to upload a malicious file ending with .png extension to masquerade as image file. This is possible only after	https://versa-networks.com/blog/versa-security-bulletin-update-on-cve-2024-39717-versa-director-dangerous-file-type-upload-vulnerability/	A-VER-VERS-030924/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a user with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin has successfully authenticated and logged in. **CVE ID: CVE-2024-39717**		
Affected Version(s): 22.1.3					
Unrestricted Upload of File with Dangerous Type	22-Aug-2024	7.2	The Versa Director GUI provides an option to customize the look and feel of the user interface. This option is only available for a user logged with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin. (Tenant level users do not have this privilege). The “Change Favicon” (Favorite Icon) option can be mis-used to upload a malicious file ending with .png extension to masquerade as image file. This is possible only after a user with Provider-Data-Center-Admin or Provider-Data-Center-System-Admin has	https://versa-networks.com/blog/versa-security-bulletin-update-on-cve-2024-39717-versa-director-dangerous-file-type-upload-vulnerability/	A-VER-VERS-030924/414

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successfully authenticated and logged in. **CVE ID: CVE-2024-39717**		
Vendor: vipre					
Product: advanced_security					
Affected Version(s): 12.0.1.214					
Improper Link Resolution Before File Access ('Link Following')	21-Aug-2024	7.8	VIPRE Advanced Security PMAgent Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Patch Management Agent. By creating a symbolic link, an attacker can abuse the agent to delete a file. An attacker can leverage this vulnerability to escalate privileges and execute	N/A	A-VIP-ADVA-030924/415

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code in the context of SYSTEM. Was ZDI-CAN-22315. **CVE ID: CVE-2024-5928**		
Uncontrolled Search Path Element	21-Aug-2024	7.8	VIPRE Advanced Security PMAgent Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Patch Management Agent. The issue results from loading a file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in	N/A	A-VIP-ADVA-030924/416

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of SYSTEM. Was ZDI-CAN-22316. **CVE ID: CVE-2024-5929**		
Incorrect Permission Assignment for Critical Resource	21-Aug-2024	7.8	VIPRE Advanced Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Anti Malware Service. The issue results from incorrect permissions on a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of	N/A	A-VIP-ADVA-030924/417

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SYSTEM. Was ZDI-CAN-22345. **CVE ID: CVE-2024-5930**		
Vendor: waspthemes					
Product: yellowpencil					
Affected Version(s): * Up to (excluding) 7.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Aug-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WaspThemes YellowPencil Visual CSS Style Editor allows Reflected XSS.This issue affects YellowPencil Visual CSS Style Editor: from n/a through 7.6.1. **CVE ID: CVE-2024-43963**	N/A	A-WAS-YELL-030924/418
Vendor: webinarpress					
Product: webinarpress					
Affected Version(s): * Up to (excluding) 1.33.21					
Cross-Site Request Forgery (CSRF)	26-Aug-2024	6.1	Cross-Site Request Forgery (CSRF) vulnerability in WebinarPress allows Cross-Site Scripting (XSS).This issue affects WebinarPress: from n/a through 1.33.20.	N/A	A-WEB-WEBI-030924/419

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43339		
Vendor: webpack.js					
Product: webpack					
Affected Version(s): * Up to (excluding) 5.94.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-2024	6.1	Webpack is a module bundler. Its main purpose is to bundle JavaScript files for usage in a browser, yet it is also capable of transforming, bundling, or packaging just about any resource or asset. The webpack developers have discovered a DOM Clobbering vulnerability in Webpack's `AutoPublicPathRuntimeModule`. The DOM Clobbering gadget in the module can lead to cross-site scripting (XSS) in web pages where scriptless attacker-controlled HTML elements (e.g., an `img` tag with an unsanitized `name` attribute) are present. Real-world exploitation of this gadget has been observed in the Canvas LMS which allows a XSS attack to happen	https://github.com/webpack/webpack/commit/955e057abc6cc83cbc3fa1e1ef67a49758bf5a61, https://github.com/webpack/webpack/security/advisories/GHSA-4vvj-4cpr-p986	A-WEB-WEBP-030924/420

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a javascript code compiled by Webpack (the vulnerable part is from Webpack). DOM Clobbering is a type of code-reuse attack where the attacker first embeds a piece of non-script, seemingly benign HTML markups in the webpage (e.g. through a post or comment) and leverages the gadgets (pieces of js code) living in the existing javascript code to transform it into executable code. This vulnerability can lead to cross-site scripting (XSS) on websites that include Webpack-generated files and allow users to inject certain scriptless HTML tags with improperly sanitized name or id attributes. This issue has been addressed in release version 5.94.0. All users are advised to upgrade. There are no known		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID: CVE-2024-43788**		
Vendor: windscribe					
Product: windscribe					
Affected Version(s): 2.9.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Aug-2024	7.8	Windscribe Directory Traversal Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Windscribe. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Windscribe Service. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in	N/A	A-WIN-WIND-030924/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of SYSTEM. Was ZDI-CAN-23441. **CVE ID: CVE-2024-6141**		
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.17					
Out-of-bounds Write	29-Aug-2024	5.5	NTLMSSP dissector crash in Wireshark 4.2.0 to 4.0.6 and 4.0.0 to 4.0.16 allows denial of service via packet injection or crafted capture file **CVE ID: CVE-2024-8250**	https://www.wireshark.org/security/wnpa-sec-2024-11.html	A-WIR-WIRE-030924/422
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.7					
Out-of-bounds Write	29-Aug-2024	5.5	NTLMSSP dissector crash in Wireshark 4.2.0 to 4.0.6 and 4.0.0 to 4.0.16 allows denial of service via packet injection or crafted capture file **CVE ID: CVE-2024-8250**	https://www.wireshark.org/security/wnpa-sec-2024-11.html	A-WIR-WIRE-030924/423
Vendor: wpbakery					
Product: page_builder					
Affected Version(s): * Up to (including) 3.0					
Improper Neutralization of Input During Web Page Generation	29-Aug-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in	N/A	A-WPB-PAGE-030924/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Classic Addons Classic Addons – WPBakery Page Builder allows Stored XSS.This issue affects Classic Addons – WPBakery Page Builder: from n/a through 3.0. **CVE ID: CVE-2024-43953**		
Vendor: wpusermanager					
Product: wp_user_manager					
Affected Version(s): * Up to (including) 2.9.10					
Cross-Site Request Forgery (CSRF)	26-Aug-2024	4.3	Cross-Site Request Forgery (CSRF) vulnerability in WP User Manager.This issue affects WP User Manager: from n/a through 2.9.10. **CVE ID: CVE-2024-43336**	N/A	A-WPU-WP_U-030924/425
Vendor: Xwiki					
Product: Xwiki					
Affected Version(s): * Up to (excluding) 14.10.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-2024	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible for a user without Script or Programming rights to craft a URL pointing to a page with arbitrary	https://github.com/xwiki/xwiki-platform/commit/27eca8423fc1ad177518077a73307682126 8509c, https://github.com/xwiki/xwiki-platform/securi	A-XWI-XWIK-030924/426

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript. This requires social engineer to trick a user to follow the URL. This has been patched in XWiki 14.10.21, 15.5.5, 15.10.6 and 16.0.0. **CVE ID: CVE-2024-43400**	ty/advisories/GHSA-wcg9-pgqv-xm5v, https://jira.xwiki.org/browse/XWIKI-21810	
Affected Version(s): * Up to (including) 15.9					
Missing Authorization	19-Aug-2024	8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A user without script/programming right can trick a user with elevated rights to edit a content with a malicious payload using a WYSIWYG editor. The user with elevated rights is not warned beforehand that they are going to edit possibly dangerous content. The payload is executed at edit time. This vulnerability has been patched in XWiki 15.10RC1. **CVE ID: CVE-2024-43401**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-f963-4cq8-2gw7, https://jira.xwiki.org/browse/XWIKI-20331, https://jira.xwiki.org/browse/XWIKI-21311, https://jira.xwiki.org/browse/XWIKI-21481, https://jira.xwiki.org/browse/XWIKI-21482	A-XWI-XWIK-030924/427
Affected Version(s): From (including) 15.0 Up to (excluding) 15.5.5					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-2024	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible for a user without Script or Programming rights to craft a URL pointing to a page with arbitrary JavaScript. This requires social engineer to trick a user to follow the URL. This has been patched in XWiki 14.10.21, 15.5.5, 15.10.6 and 16.0.0. **CVE ID: CVE-2024-43400**	https://github.com/xwiki/xwiki-platform/commit/27eca8423fc1ad177518077a733076821268509c, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-wcg9-pgqv-xm5v, https://jira.xwiki.org/browse/XWIKI-21810	A-XWI-XWIK-030924/428
Affected Version(s): From (including) 15.6 Up to (excluding) 15.10.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Aug-2024	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible for a user without Script or Programming rights to craft a URL pointing to a page with arbitrary JavaScript. This requires social engineer to trick a user to follow the URL. This has been patched in XWiki 14.10.21, 15.5.5, 15.10.6 and 16.0.0.	https://github.com/xwiki/xwiki-platform/commit/27eca8423fc1ad177518077a733076821268509c, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-wcg9-pgqv-xm5v, https://jira.xwiki.org/browse/XWIKI-21810	A-XWI-XWIK-030924/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43400		
Vendor: yzncms					
Product: yzncms					
Affected Version(s): 1.4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Aug-2024	5.4	A cross-site scripting (XSS) vulnerability in the component /index/index.html of YZNCMS v1.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the configured remarks text field. **CVE ID: CVE-2024-42939**	N/A	A-YZN-YZNC-030924/430
Vendor: zaytech					
Product: smart_online_order_for_clover					
Affected Version(s): * Up to (excluding) 1.5.7					
Missing Authorization	21-Aug-2024	6.5	The Smart Online Order for Clover plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'moo_deactivateAndClean' function in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated attackers to deactivate the	N/A	A-ZAY-SMAR-030924/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin and drop all plugin tables from the database. **CVE ID: CVE-2024-7032**		
Missing Authorization	21-Aug-2024	4.3	The Smart Online Order for Clover plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.5.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update product and category descriptions, category titles and images, and sort order. **CVE ID: CVE-2024-7030**	N/A	A-ZAY-SMAR-030924/432
Vendor: Zen-cart					
Product: zen_cart					
Affected Version(s): 1.5.8a					
Inclusion of Functionality from Untrusted	21-Aug-2024	8.1	Zen Cart findPluginAdminPage Local File Inclusion Remote Code Execution Vulnerability. This vulnerability	N/A	A-ZEN-ZEN_-030924/433

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Control Sphere			allows remote attackers to execute arbitrary code on affected installations of Zen Cart. Authentication is not required to exploit this vulnerability. The specific flaw exists within the findPluginAdminPage function. The issue results from the lack of proper validation of user-supplied data prior to passing it to a PHP include function. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the service account. Was ZDI-CAN-21408. **CVE ID: CVE-2024-5762**		
Vendor: zephyr-one					
Product: zephyr_project_manager					
Affected Version(s): * Up to (excluding) 3.3.103					
Improper Neutralization of Input During Web Page	26-Aug-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site	N/A	A-ZEP-ZEPH-030924/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting') vulnerability in Dylan James Zephyr Project Manager allows Reflected XSS.This issue affects Zephyr Project Manager: from n/a through .3.102. **CVE ID: CVE-2024-43915**		
Vendor: Zoho					
Product: manageengine_remote_monitoring_and_management					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the deploy agent option. **CVE ID: CVE-2024-5466**	https://www.manageengine.com/itom/advisory/cve-2024-5466.html	A-ZOH-MANA-030924/435
Vendor: Zohocorp					
Product: manageengine_adaudit_plus					
Affected Version(s): 8.1					
Improper Neutralization of Special Elements used in an	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL	https://www.manageengine.com/products/active-directory-audit/cve-2024-5467.html	A-ZOH-MANA-030924/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			injection in account lockout report. **CVE ID: CVE-2024-5467**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL injection in extranet lockouts report option. **CVE ID: CVE-2024-5586**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/437
Affected Version(s): * Up to (excluding) 8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in file summary option. **CVE ID: CVE-2024-36514**	https://www.manageengine.com/products/active-directory-audit/cve-2024-36514.html	A-ZOH-MANA-030924/438
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in dashboard. Note: This vulnerability is different from another vulnerability (CVE-2024-36516), both	https://www.manageengine.com/products/active-directory-audit/cve-2024-36515.html	A-ZOH-MANA-030924/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of which have affected ADAudit Plus' dashboard. **CVE ID: CVE-2024-36515**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in dashboard. Note: This vulnerability is different from another vulnerability (CVE-2024-36515), both of which have affected ADAudit Plus' dashboard. **CVE ID: CVE-2024-36516**	https://www.manageengine.com/products/active-directory-audit/cve-2024-36516.html	A-ZOH-MANA-030924/440
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in alerts module. **CVE ID: CVE-2024-36517**	https://www.manageengine.com/products/active-directory-audit/cve-2024-36517.html	A-ZOH-MANA-030924/441
Improper Neutralization of Special Elements used in an SQL Command	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in	https://www.manageengine.com/products/active-directory-audit/cve-2024-5490.html	A-ZOH-MANA-030924/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			aggregate reports option. **CVE ID: CVE-2024-5490**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in reports module. **CVE ID: CVE-2024-5556**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5556.html	A-ZOH-MANA-030924/443
Affected Version(s): * Up to (including) 8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL injection in account lockout report. **CVE ID: CVE-2024-5467**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5467.html	A-ZOH-MANA-030924/444
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL injection in extranet lockouts report option. **CVE ID: CVE-2024-5586**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/445
Product: manageengine_opmanager					
Affected Version(s): * Up to (including) 12.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the deploy agent option. **CVE ID: CVE-2024-5466**	https://www.manageengine.com/itom/advisory/cve-2024-5466.html	A-ZOH-MANA-030924/446
Affected Version(s): 12.8					
Improper Control of Generation of Code ('Code Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the deploy agent option. **CVE ID: CVE-2024-5466**	https://www.manageengine.com/itom/advisory/cve-2024-5466.html	A-ZOH-MANA-030924/447
Product: manageengine_opmanager_msp					
Affected Version(s): * Up to (including) 12.7					
Improper Control of Generation of Code ('Code Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329	https://www.manageengine.com/itom/advisory/cve-2024-5466.html	A-ZOH-MANA-030924/448

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and below are vulnerable to the authenticated remote code execution in the deploy agent option. **CVE ID: CVE-2024-5466**		
Affected Version(s): 12.8					
Improper Control of Generation of Code ('Code Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the deploy agent option. **CVE ID: CVE-2024-5466**	https://www.manageengine.com/itom/advisory/cve-2024-5466.html	A-ZOH-MANA-030924/449
Product: manageengine_opmanager_plus					
Affected Version(s): * Up to (including) 12.7					
Improper Control of Generation of Code ('Code Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the	https://www.manageengine.com/itom/advisory/cve-2024-5466.html	A-ZOH-MANA-030924/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deploy agent option. **CVE ID: CVE-2024-5466**		
Affected Version(s): 12.8					
Improper Control of Generation of Code ('Code Injection')	23-Aug-2024	8.8	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the deploy agent option. **CVE ID: CVE-2024-5466**	https://www.manageengine.com/itom/advisory/cve-2024-5466.html	A-ZOH-MANA-030924/451
Product: manageengine_servicedesk_plus					
Affected Version(s): * Up to (including) 14.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	6.1	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter	https://www.manageengine.com/products/service-desk/CVE-2024-41150.html	A-ZOH-MANA-030924/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus: through 14800. **CVE ID: CVE-2024-41150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25. **CVE ID: CVE-2024-38869**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/453
Affected Version(s): 14.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	6.1	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter	https://www.manageengine.com/products/service-desk/CVE-2024-41150.html	A-ZOH-MANA-030924/454

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus: through 14800. **CVE ID: CVE-2024-41150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25. **CVE ID: CVE-2024-38869**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/455
Product: manageengine_servicedesk_plus_msp					
Affected Version(s): * Up to (including) 14.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	6.1	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter	https://www.manageengine.com/products/service-desk/CVE-2024-41150.html	A-ZOH-MANA-030924/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus: through 14800. **CVE ID: CVE-2024-41150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25. **CVE ID: CVE-2024-38869**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/457
Affected Version(s): 14.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	6.1	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter	https://www.manageengine.com/products/service-desk/CVE-2024-41150.html	A-ZOH-MANA-030924/458

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus: through 14800. **CVE ID: CVE-2024-41150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25. **CVE ID: CVE-2024-38869**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/459
Product: manageengine_supportcenter_plus					
Affected Version(s): * Up to (including) 14.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	6.1	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter	https://www.manageengine.com/products/service-desk/CVE-2024-41150.html	A-ZOH-MANA-030924/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus: through 14800. **CVE ID: CVE-2024-41150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25. **CVE ID: CVE-2024-38869**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/461
Affected Version(s): 14.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	6.1	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter	https://www.manageengine.com/products/service-desk/CVE-2024-41150.html	A-ZOH-MANA-030924/462

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus: through 14800. **CVE ID: CVE-2024-41150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Aug-2024	5.4	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25. **CVE ID: CVE-2024-38869**	https://www.manageengine.com/products/active-directory-audit/cve-2024-5586.html	A-ZOH-MANA-030924/463
Vendor: zzcms					
Product: zzcms					
Affected Version(s): 2023					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Aug-2024	7.5	A vulnerability was found in ZZCMS 2023. It has been declared as critical. This vulnerability affects unknown code of the file /I/list.php. The manipulation of the argument skin leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to	N/A	A-ZZC-ZZCM-030924/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. **CVE ID: CVE-2024-7924**		
N/A	19-Aug-2024	7.5	A vulnerability was found in ZZCMS 2023. It has been rated as problematic. This issue affects some unknown processing of the file 3/E_bak5.1/upload/eginfo.php. The manipulation of the argument phome with the input ShowPHPInfo leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-7925**	N/A	A-ZZC-ZZCM-030924/465
Hardware					
Vendor: autel					
Product: maxicharger_ac_elite_business_c50					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Aug-2024	8.8	Autel MaxiCharger AC Elite Business C50 AppAuthenExchangeRandomNum Stack-Based Buffer Overflow Remote Code Execution	N/A	H-AUT-MAXI-030924/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the AppAuthenExchangeRandomNum BLE command. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23384. **CVE ID: CVE-2024-7795**		
Vendor: Dell					
Product: dnr-202l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNR--030924/467

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dnr-322l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_c	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNR--030924/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ontent/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dnr-326					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNR--030924/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		

Product: dns-1100-4

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-120					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_li	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			st/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-1200-05					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/472

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dns-1550-04					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/473

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-315l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cg	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			i_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-320					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/475

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7922		
Product: dns-320l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-320lw					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltrac	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/477

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-321					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')		🟥	DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-323					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/479

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-325					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/c	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/480

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-326					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/481

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')		🟥	322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-327l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-340l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/c	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/483

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-343					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publicati	H-DEL-DNS--030924/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')		🟥	DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-345					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/485

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-726-4					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DEL-DNS--030924/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Vendor: Dlink					
Product: dir-846w					
Affected Version(s): a1					
Improper Neutralization of	27-Aug-2024	9.8	D-Link DIR-846W A1 FW100A43 was discovered to	N/A	H-DLI-DIR--030924/487

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			contain a remote command execution (RCE) vulnerability via the tomography_ping_address parameter in /HNAP1/ interface. **CVE ID: CVE-2024-41622**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the lan(0)_dhcps_staticlist parameter. This vulnerability is exploited via a crafted POST request. **CVE ID: CVE-2024-44341**	N/A	H-DLI-DIR--030924/488
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the wl(0).(0)_ssid parameter. This vulnerability is exploited via a crafted POST request. **CVE ID: CVE-2024-44342**	N/A	H-DLI-DIR--030924/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	8.8	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via keys smartqos_express_devices and smartqos_normal_devices in SetSmartQoSSettings. **CVE ID: CVE-2024-44340**	N/A	H-DLI-DIR--030924/490
Product: di_8004w					
Affected Version(s): -					
N/A	23-Aug-2024	9.8	D-Link DI_8004W 16.07.26A1 contains a command execution vulnerability in jhttpd msp_info_htm function. **CVE ID: CVE-2024-44381**	https://www.dlink.com/en/security-bulletin/	H-DLI-DI_8-030924/491
N/A	23-Aug-2024	9.8	D-Link DI_8004W 16.07.26A1 contains a command execution vulnerability in the jhttpd upgrade_filter_asp function. **CVE ID: CVE-2024-44382**	N/A	H-DLI-DI_8-030924/492
Product: dnr-202l					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/493

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/494

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/496

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNR--030924/498

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		🟥	DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/499

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/501

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/503

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/504

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dnr-322l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/507

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/508

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/509

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNR--030924/510

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		🟥	DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/512

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/513

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/514

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/515

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNR--030924/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')		🟥	DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8212		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/517

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/518

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dnr-326					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/520

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/521

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralizat	24-Aug-2024	9.8	A vulnerability has been found in D-	https://support announcement.	H-DLI-DNR--030924/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/523

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/524

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/525

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/526

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability was found in D-Link	https://support announcement.	H-DLI-DNR--030924/528

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/529

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--030924/531

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-1100-4					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/532

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/533

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability, which was classified as critical,	https://supportannouncement.us.dlink.com/se	H-DLI-DNS--030924/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/536

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.c	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/538

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8134		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/540

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/541

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/543

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/544

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-120					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNS--030924/546

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		🟥	D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/547

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/548

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/549

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/550

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8133		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/553

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/554

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/557

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-1200-05					
Affected Version(s): -					
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	H-DLI-DNS--030924/558

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/562

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/563

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8132		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/565

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/566

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_Di	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/567

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/568

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	H-DLI-DNS--030924/570

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-1550-04					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/572

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/573

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8131		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/576

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/578

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/581

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability classified as critical	https://support announcement.	H-DLI-DNS--030924/582

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/583

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-315l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/584

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8130		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/588

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/590

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/591

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/592

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://support announcement. us.dlink.com/se curity/publicati	H-DLI-DNS--030924/593

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8211		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/594

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/596

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-320					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/597

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/599

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8129		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/600

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/601

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/603

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/604

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability was found in D-Link	https://support announcement.	H-DLI-DNS--030924/605

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8210		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/608

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-320l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/610

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/611

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/612

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/613

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/616

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-	https://supportannouncement.us.dlink.com/se	H-DLI-DNS--030924/617

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/620

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/621

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/622

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-320lw					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/624

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/625

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/626

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/627

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/628

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNS--030924/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		🟥	DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/632

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/633

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/634

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/635

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-321					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/636

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/638

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/639

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNS--030924/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8132		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/642

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/644

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_Di	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/646

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	H-DLI-DNS--030924/648

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-323					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/652

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8131		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/654

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/657

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/659

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability classified as critical	https://support announcement.	H-DLI-DNS--030924/660

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/661

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-325					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/663

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/664

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/665

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8130		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/666

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/667

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/668

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/669

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/670

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNS--030924/671

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8211		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/672

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-326					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/675

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/676

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/677

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8129		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/678

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/680

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/681

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability was found in D-Link	https://support announcement.	H-DLI-DNS--030924/683

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	us.dlink.com/security/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8210		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/684

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/687

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-327l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/688

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/690

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/691

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/692

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/694

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-	https://supportannouncement.us.dlink.com/se	H-DLI-DNS--030924/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/696

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/698

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/699

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-340l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/701

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/702

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/704

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/706

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNS--030924/707

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		🟥	DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/709

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/710

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/711

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/712

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-343					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/714

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://support announcement. us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	H-DLI-DNS--030924/719

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8132		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/720

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/722

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_Di	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	H-DLI-DNS--030924/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-345					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/727

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/728

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/729

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/730

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8131		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/732

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/734

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/735

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/737

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability classified as critical	https://support announcement.	H-DLI-DNS--030924/738

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-726-4					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/740

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/741

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8130		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/744

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/745

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/746

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/747

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/748

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://support announcement. us.dlink.com/se curity/publicati	H-DLI-DNS--030924/749

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8211		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/751

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--030924/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Vendor: fastcom					
Product: fw300r					
Affected Version(s): -					
Out-of-bounds Write	26-Aug-2024	9.8	A stack overflow in FAST FW300R v1.3.13 Build 141023 Rel.61347n allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via a crafted file path. **CVE ID: CVE-2024-41285**	N/A	H-FAS-FW30-030924/753
Vendor: Google					
Product: nest_mini					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Aug-2024	5.9	The libcurl CURLOPT_SSL_VERIFYPEER option was disabled on a subset of requests made by Nest production devices which enabled a potential man-in-the-middle attack on requests to Google cloud services by any host the traffic was routed through. **CVE ID: CVE-2024-32928**	https://support.google.com/product-documentation/answer/14771247?hl=en&ref_topic=12974021&sjid=9111851316942032590-NA#zippy=	H-GOO-NEST-030924/754
Vendor: Linksys					
Product: e1500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Aug-2024	8.8	A Command Injection vulnerability exists in the do_upgrade_post function of the httpd binary in Linksys E1500 v1.0.06.001. As a result, an authenticated attacker can execute OS commands with root privileges. **CVE ID: CVE-2024-42633**	N/A	H-LIN-E150-030924/755
Vendor: nepstech					
Product: ntpl-xpon1gfevn					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Aug-2024	9.8	An issue in wishnet Nepstech Wifi Router NTPL-XPON1GFEVN v1.0 allows a remote attacker to obtain sensitive information via the cookie's parameter **CVE ID: CVE-2024-42658**	N/A	H-NEP-NTPL-030924/756
Missing Encryption of Sensitive Data	19-Aug-2024	7.5	An issue in wishnet Nepstech Wifi Router NTPL-XPON1GFEVN v1.0 allows a remote attacker to obtain sensitive information via the lack of encryption during login process **CVE ID: CVE-2024-42657**	N/A	H-NEP-NTPL-030924/757
Vendor: nissan-global					
Product: altima					
Affected Version(s): 2022					
Use of Insufficiently Random Values	19-Aug-2024	7.5	Predictable seed generation in the security access mechanism of UDS in the Blind Spot Protection Sensor ECU in Nissan Altima (2022) allows attackers to predict the requested seeds and bypass security controls via repeated ECU	N/A	H-NIS-ALTI-030924/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resets and seed requests. **CVE ID: CVE-2024-6348**		
Vendor: ruijie					
Product: eg2000k					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	26-Aug-2024	4.9	A vulnerability has been found in Ruijie EG2000K 11.1(6)B2 and classified as critical. This vulnerability affects unknown code of the file /tool/index.php?c=download&a=save. The manipulation of the argument content leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8166**	N/A	H-RUI-EG20-030924/759
Vendor: teldat					
Product: rs123					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-2024	4.8	Cross Site Scripting vulnerability in Teldats Router RS123, RS123w allows attacker to execute arbitrary code via the cmdcookie parameter to the upgrade/query.php page. **CVE ID: CVE-2022-39996**	N/A	H-TEL-RS12-030924/760
Product: rs123w					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-2024	4.8	Cross Site Scripting vulnerability in Teldats Router RS123, RS123w allows attacker to execute arbitrary code via the cmdcookie parameter to the upgrade/query.php page. **CVE ID: CVE-2022-39996**	N/A	H-TEL-RS12-030924/761
Vendor: tencacn					
Product: fh1206					
Affected Version(s): -					
Out-of-bounds Write	23-Aug-2024	8.8	Tenda FH1206 V1.2.0.8(8155)_EN contains a Buffer Overflow vulnerability via the function formWrlsafeset. **CVE ID: CVE-2024-44390**	N/A	H-TEN-FH12-030924/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Aug-2024	6.5	Tenda FH1206 V1.2.0.8(8155)_EN contains a Buffer Overflow vulnerability via the functino formWrlExtraGet. **CVE ID: CVE-2024-44387**	N/A	H-TEN-FH12-030924/763
Vendor: Tenda					
Product: ax1806					
Affected Version(s): -					
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo. **CVE ID: CVE-2024-44563**	N/A	H-TEN-AX18-030924/764
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the serverName parameter in the function form_fast_setting_internet_set. **CVE ID: CVE-2024-44565**	N/A	H-TEN-AX18-030924/765
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo.	N/A	H-TEN-AX18-030924/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-44556		
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function setIptvInfo. **CVE ID: CVE-2024-44558**	N/A	H-TEN-AX18-030924/767
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv. **CVE ID: CVE-2024-44549**	N/A	H-TEN-AX18-030924/768
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv. **CVE ID: CVE-2024-44550**	N/A	H-TEN-AX18-030924/769
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv. **CVE ID: CVE-2024-44551**	N/A	H-TEN-AX18-030924/770
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via	N/A	H-TEN-AX18-030924/771

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the adv.iptv.stballvlans parameter in the function formGetIptv. **CVE ID: CVE-2024-44552**		
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv. **CVE ID: CVE-2024-44553**	N/A	H-TEN-AX18-030924/772
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo. **CVE ID: CVE-2024-44555**	N/A	H-TEN-AX18-030924/773
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo. **CVE ID: CVE-2024-44557**	N/A	H-TEN-AX18-030924/774
Product: g3					
Affected Version(s): -					
Out-of-bounds Write	27-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda G3	N/A	H-TEN-G3-030924/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.11.0.20. This issue affects the function formSetDebugCfg of the file /goform/setDebugCfg. The manipulation of the argument enable/level/module leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8224**		
Out-of-bounds Write	27-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda G3 15.11.0.20. Affected is the function formSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument sysTimePolicy leads to stack-based buffer	N/A	H-TEN-G3-030924/776

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8225**		
Product: o1					
Affected Version(s): -					
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability has been found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this	N/A	H-TEN-O1-030924/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure but did not respond in any way. **CVE ID: CVE-2024-8226**		
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this issue is the function fromDhcpSetSer of the file /goform/DhcpSetSer. The manipulation of the argument dhcpStartIp/dhcpEndIp/dhcpGw/dhcpMask/dhcpLeaseTime/dhcpDns1/dhcpDns2 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8227**	N/A	H-TEN-O1-030924/778
Product: o5					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O5 1.0.0.8(5017). It has been classified as critical. This affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8228**	N/A	H-TEN-O5-030924/779
Product: o6					
Affected Version(s): -					
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been declared as critical. This vulnerability affects the function frommacFilterModify of the file /goform/operateM	N/A	H-TEN-O6-030924/780

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			acFilter. The manipulation of the argument mac leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8229**		
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been rated as critical. This issue affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was	N/A	H-TEN-O6-030924/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8230**		
Vendor: totolink					
Product: a3002r					
Affected Version(s): -					
Out-of-bounds Write	28-Aug-2024	9.8	TOTOLINK AC1200 Wireless Router A3002R Firmware V1.1.1-B20200824 is vulnerable to Buffer Overflow. In the boa server program's CGI handling function formWlEncrypt, there is a lack of length restriction on the wlan_ssid field. This oversight leads to potential buffer overflow under specific circumstances. For instance, by invoking the formWlanRedirect function with specific parameters to alter wlan_idx's value and subsequently invoking the formWlEncrypt function, an attacker can trigger buffer overflow, enabling arbitrary	N/A	H-TOT-A300-030924/782

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command execution or denial of service attacks. **CVE ID: CVE-2024-34195**		
Product: ac1200_t8					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Aug-2024	9.8	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228 and classified as critical. Affected by this vulnerability is the function setDiagnosisCfg. The manipulation leads to os command injection. The attack can be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8075**	N/A	H-TOT-AC12-030924/783
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228 and classified as critical. Affected by this issue is the function setDiagnosisCfg. The manipulation leads to buffer	N/A	H-TOT-AC12-030924/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. The attack may be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8076**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been classified as critical. This affects the function setTracerouteCfg. The manipulation leads to os command injection. It is possible to initiate the attack remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8077**	N/A	H-TOT-AC12-030924/785
Buffer Copy without Checking Size of Input ('Classic	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been declared as critical. This vulnerability affects the function setTracerouteCfg.	N/A	H-TOT-AC12-030924/786

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			The manipulation leads to buffer overflow. The attack can be initiated remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8078**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been rated as critical. This issue affects the function exportOvpn. The manipulation leads to buffer overflow. The attack may be initiated remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8079**	N/A	H-TOT-AC12-030924/787
Product: ex1200l					
Affected Version(s): -					
Out-of-bounds Write	18-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in TOTOLINK EX1200L	N/A	H-TOT-EX12-030924/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.3.5u.6146_B20201023. Affected is the function setDefResponse of the file /www/cgi-bin/cstecgi.cgi. The manipulation of the argument IpAddress 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. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7908**		
Out-of-bounds Write	18-Aug-2024	9.8	A vulnerability has been found in TOTOLINK EX1200L 9.3.5u.6146_B20201023 and classified as critical. Affected by this vulnerability is the function setLanguageCfg of the file /www/cgi-bin/cstecgi.cgi. The manipulation of the argument langType leads to stack-based buffer	N/A	H-TOT-EX12-030924/789

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7909**		
Product: t10					
Affected Version(s): -					
Use of Hard-coded Credentials	26-Aug-2024	9.8	A vulnerability classified as critical has been found in TOTOLINK T10 AC1200 4.1.8cu.5207. Affected is an unknown function of the file /squashfs-root/web_cste/cgi-bin/product.ini of the component Telnet Service. The manipulation leads to hard-coded credentials. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early	N/A	H-TOT-T10-030924/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8162**		
Product: x6000r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in TOTOLINK X6000R 9.4.0cu.852_20230719. This issue affects the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument rtLogServer leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7907**	N/A	H-TOT-X600-030924/791
Operating System					
Vendor: 3DS					
Product: 3dexperience					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) r2022x Up to (including) r2024x					
URL Redirection to Untrusted Site ('Open Redirect')	20-Aug-2024	6.1	An URL redirection to untrusted site (open redirect) vulnerability affecting 3DPassport in 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to redirect users to an arbitrary website via a crafted URL. **CVE ID: CVE-2024-6377**	https://www.3ds.com/vulnerability/advisories	O-3DS-3DEX-030924/792
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Aug-2024	6.1	A reflected Cross-site Scripting (XSS) vulnerability affecting 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-6379**	https://www.3ds.com/vulnerability/advisories	O-3DS-3DEX-030924/793
Improper Neutralization of Input During Web Page	20-Aug-2024	5.4	A reflected Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative	https://www.3ds.com/vulnerability/advisories	O-3DS-3DEX-030924/794

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session. **CVE ID: CVE-2024-6378**		
Vendor: autel					
Product: maxicharger_ac_elite_business_c50_firmware					
Affected Version(s): * Up to (excluding) 1.36.00					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Aug-2024	8.8	Autel MaxiCharger AC Elite Business C50 AppAuthenExchangeRandomNum Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the	N/A	O-AUT-MAXI-030924/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AppAuthenExchangeRandomNum BLE command. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23384. **CVE ID: CVE-2024-7795**		
Vendor: Dell					
Product: dnr-202l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNR--030924/796

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dnr-322l_firmware					
Affected Version(s): -					
Improper Neutralization of Special	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	O-DEL-DNR--030924/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')		🟥	DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dnr-326_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNR--030924/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-1100-4_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-1200-05_firmware					
Affected Version(s): -					
Improper Neutralization of	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-	https://supportannouncement.us.dlink.com/se	O-DEL-DNS--030924/800

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')		🟥	202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-120_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-1550-04_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-315l_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/803

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-320lw_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_c	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/804

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ontent/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-320l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-320_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/806

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-321_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_li	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			st/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-323_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dns-325_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/809

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-326_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cg	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			i_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-327l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/811

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-7922		
Product: dns-340l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-343_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltrac	https://support announcement. us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-345_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/814

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')		🟥	DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-7922**		
Product: dns-726-4_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DEL-DNS--030924/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-7922**		
Vendor: Dlink					
Product: dir-846w_firmware					
Affected Version(s): fw100a43					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the tomography_ping_address parameter in /HNAP1/ interface. **CVE ID: CVE-2024-41622**	N/A	O-DLI-DIR--030924/816
Improper Neutralization of Special Elements used in an	27-Aug-2024	9.8	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE)	N/A	O-DLI-DIR--030924/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			vulnerability via the lan(0)_dhcps_staticlist parameter. This vulnerability is exploited via a crafted POST request. **CVE ID: CVE-2024-44341**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the wl(0).(0)_ssid parameter. This vulnerability is exploited via a crafted POST request. **CVE ID: CVE-2024-44342**	N/A	O-DLI-DIR--030924/818
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	8.8	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via keys smartqos_express_devices and smartqos_normal_devices in SetSmartQoSSettings. **CVE ID: CVE-2024-44340**	N/A	O-DLI-DIR--030924/819
Product: di_8004w_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 16.07.26a1					
N/A	23-Aug-2024	9.8	D-Link DI_8004W 16.07.26A1 contains a command execution vulnerability in jhttpd msp_info_htm function. **CVE ID: CVE-2024-44381**	https://www.dlink.com/en/security-bulletin/	O-DLI-DI_8-030924/820
N/A	23-Aug-2024	9.8	D-Link DI_8004W 16.07.26A1 contains a command execution vulnerability in the jhttpd upgrade_filter_asp function. **CVE ID: CVE-2024-44382**	N/A	O-DLI-DI_8-030924/821
Product: dnr-202l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/822

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/823

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralizat	24-Aug-2024	9.8	A vulnerability, which was	https://support announcement.	O-DLI-DNR--030924/824

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	us.dlink.com/security/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/825

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/826

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/827

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/828

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNR--030924/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8134		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/830

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/832

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/833

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/834

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dnr-322l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/835

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNR--030924/836

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/841

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')		🟥	322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8133		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/842

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/844

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/845

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dnr-326_firmware					
Affected Version(s): -					
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	O-DLI-DNR--030924/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/849

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/851

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')		🟥	322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8132		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/855

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/856

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_Di	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/857

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/858

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--030924/859

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	O-DLI-DNR--030924/860

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-1100-4_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/862

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/863

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/865

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8131		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/866

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/867

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/868

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/869

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://support announcement. us.dlink.com/se curity/publicati on.aspx?name= SAP10383	O-DLI-DNS--030924/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability classified as critical	https://support announcement.	O-DLI-DNS--030924/872

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/873

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-1200-05_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/875

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/876

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8130		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/878

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/880

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/881

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8211		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/884

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/885

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/886

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-120_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/887

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8129		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/890

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/891

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/892

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/893

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/894

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability was found in D-Link	https://support announcement.	O-DLI-DNS--030924/895

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8210		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/896

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/897

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/898

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-1550-04_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/900

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/902

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/903

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/905

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-	https://support announcement. us.dlink.com/se	O-DLI-DNS--030924/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/908

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/909

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/910

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/911

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/912

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-315l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/914

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/915

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/916

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/917

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/918

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/919

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/920

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/921

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/922

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/923

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/924

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/925

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-320lw_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/926

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/928

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/929

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/930

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/931

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8132		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/932

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/933

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_Di	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/935

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/936

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	O-DLI-DNS--030924/938

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-320l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/940

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/941

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/942

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/943

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8131		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/945

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/947

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/948

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/949

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability classified as critical	https://support announcement.	O-DLI-DNS--030924/950

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-320_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/952

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/954

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8130		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/956

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/957

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/958

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/961

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8211		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/963

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-321_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/967

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8129		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/968

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/970

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/971

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability was found in D-Link	https://support announcement.	O-DLI-DNS--030924/973

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')		🟥	DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	us.dlink.com/security/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8210		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/974

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/976

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/977

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-323_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/979

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/980

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/981

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/982

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/983

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-	https://supportannouncement.us.dlink.com/se	O-DLI-DNS--030924/985

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/987

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/988

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/989

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-325_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/992

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/993

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/994

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/995

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/996

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/998

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1002

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1003

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')		🟥	323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-326_firmware					
Affected Version(s): -					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1004

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1005

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1006

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1007

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8132		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1010

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1011

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_Di	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			skMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1014

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-	https://supportannouncement.us.dlink.com/se	O-DLI-DNS--030924/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-327l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1017

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1018

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1019

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1020

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8131		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1022

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability classified as critical	https://support announcement.	O-DLI-DNS--030924/1028

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1029

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-340l_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1030

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1032

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8130		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE:	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1034

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1036

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/1039

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	on.aspx?name=SAP10383	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8211		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1040

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1041

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-343_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1044

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1045

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')		🟥	315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8129		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1046

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1047

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1048

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralizat	27-Aug-2024	9.8	A vulnerability was found in D-Link	https://support announcement.	O-DLI-DNS--030924/1051

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	us.dlink.com/security/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-8210		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1052

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1053

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-345_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1056

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1057

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1058

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_Spare Dsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-	https://supportannouncement.us.dlink.com/se	O-DLI-DNS--030924/1063

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')		🟥	202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	curity/publication.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1064

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1066

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1068

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Product: dns-726-4_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	24-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')		🟥	DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8127**		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1070

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8128**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1071

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8129**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1072

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument f_a_key leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8130**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_module_name leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8131**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345,	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1074

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8132**		
Improper Neutralization of Special	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L,	https://supportannouncement.us.dlink.com/security/publicati	O-DLI-DNS--030924/1075

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		🟥	DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be	on.aspx?name=SAP10383	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retired and replaced. **CVE ID: CVE-2024-8133**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1076

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8134**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1077

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8210**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8211**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Aug-2024	9.8	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8212**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Aug-2024	9.8	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1080

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8213**		
Improper Neutralization of Special Elements used in an OS Command ('OS	27-Aug-2024	9.8	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--030924/1081

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. **CVE ID: CVE-2024-8214**		
Vendor: fastcom					
Product: fw300r_firmware					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.3.13_build_141023_rel.61347n					
Out-of-bounds Write	26-Aug-2024	9.8	A stack overflow in FAST FW300R v1.3.13 Build 141023 Rel.61347n allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via a crafted file path. **CVE ID: CVE-2024-41285**	N/A	O-FAS-FW30-030924/1082
Vendor: Google					
Product: android					
Affected Version(s): -					
Use After Free	21-Aug-2024	8.8	Use after free in Passwords in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2024-7964**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	O-GOO-ANDR-030924/1083
Use After Free	19-Aug-2024	7.8	In sendDeviceState_1_6 of RadioExt.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/pixel/2024-08-01	O-GOO-ANDR-030924/1084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID: CVE-2024-32927**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Aug-2024	6.1	Microsoft Edge for Android Spoofing Vulnerability **CVE ID: CVE-2024-38208**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38208	O-GOO-ANDR-030924/1085
N/A	21-Aug-2024	4.3	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID: CVE-2024-8034**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	O-GOO-ANDR-030924/1086
Product: nest_mini_firmware					
Affected Version(s): -					
N/A	19-Aug-2024	5.9	The libcurl CURLOPT_SSL_VERIFYPEER option was disabled on a subset of requests made by Nest production devices which enabled a potential man-in-	https://support.google.com/product-documentation/answer/14771247?hl=en&ref_topic=12974021&sjid=9111851	O-GOO-NEST-030924/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the-middle attack on requests to Google cloud services by any host the traffic was routed through. **CVE ID: CVE-2024-32928**	316942032590-NA#zippy=	
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Use of a Broken or Risky Cryptographic Algorithm	22-Aug-2024	7.5	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-39745**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297312, https://www.ibm.com/support/pages/node/7166195	O-IBM-AIX-030924/1088
Missing Encryption of Sensitive Data	22-Aug-2024	5.9	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using	https://exchange.xforce.ibmcloud.com/vulnerabilities/297313, https://www.ibm.com/support/pages/node/7166018	O-IBM-AIX-030924/1089

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			man in the middle techniques. **CVE ID: CVE-2024-39746**		
Cross-Site Request Forgery (CSRF)	22-Aug-2024	4.3	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID: CVE-2024-39744**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297236, https://www.ibm.com/support/pages/node/7166196	O-IBM-AIX-030924/1090
Vendor: Linksys					
Product: e1500_firmware					
Affected Version(s): 1.0.06.001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Aug-2024	8.8	A Command Injection vulnerability exists in the do_upgrade_post function of the httpd binary in Linksys E1500 v1.0.06.001. As a result, an authenticated attacker can execute OS commands with root privileges. **CVE ID: CVE-2024-42633**	N/A	O-LIN-E150-030924/1091
Vendor: Linux					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: linux_kernel					
Affected Version(s): -					
Use of a Broken or Risky Cryptographic Algorithm	22-Aug-2024	7.5	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-39745**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297312, https://www.ibm.com/support/pages/node/7166195	O-LIN-LINU-030924/1092
Externally Controlled Reference to a Resource in Another Sphere	27-Aug-2024	6.7	In certain highly specific configurations of the host system and MongoDB server binary installation on Linux Operating Systems, it may be possible for a unintended actor with host-level access to cause the MongoDB Server binary to load unintended actor-controlled shared libraries when the server binary is started, potentially resulting in the unintended actor gaining full control over the MongoDB server process. This issue affects MongoDB Server v5.0 versions prior	https://jira.mongodb.org/browse/SERVER-69507	O-LIN-LINU-030924/1093

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 5.0.14 and MongoDB Server v6.0 versions prior to 6.0.3. Required Configuration: Only environments with Linux as the underlying operating system is affected by this issue **CVE ID: CVE-2024-8207**		
Missing Encryption of Sensitive Data	22-Aug-2024	5.9	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **CVE ID: CVE-2024-39746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297313, https://www.ibm.com/support/pages/node/7166018	O-LIN-LINU-030924/1094
Cross-Site Request Forgery (CSRF)	22-Aug-2024	4.3	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-site request forgery	https://exchange.xforce.ibmcloud.com/vulnerabilities/297236, https://www.ibm.com/support	O-LIN-LINU-030924/1095

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID: CVE-2024-39744**	/pages/node/7166196	
Affected Version(s): * Up to (excluding) 4.19.316					
Use After Free	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unregister flowtable hooks on netns exit Unregister flowtable hooks before they are releases via nf_tables_flowtable_destroy() otherwise hook core reports UAF. BUG: KASAN: use-after-free in nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 Read of size 4 at addr ffff8880736f7438	https://git.kernel.org/stable/c/6069da443bf65f513bb507bb21e2f87cfb1ad0b6, https://git.kernel.org/stable/c/88c795491bf45a8c08a0f94c9ca4f13722e51013, https://git.kernel.org/stable/c/8ffb8ac3448845f65634889b051bd65e4dee484b	O-LIN-LINU-030924/1096

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by task syz-executor579/3666 CPU: 0 PID: 3666 Comm: syz-executor579 Not tainted 5.16.0-rc5-syzkaller #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 lib/dump_stack.c:88 [inline] lib/dump_stack.c:106 dump_stack_lvl+0x1dc/0x2d8 lib/dump_stack.c:106 lib/dump_stack.c:106 print_address_description+0x65/0x380 mm/kasan/report.c:247 mm/kasan/report.c:247		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kasan_report mm/kasan/report.c:433 [inline] __kasan_report mm/kasan/report.c:433 [inline] mm/kasan/report.c:450 kasan_report+0x19a/0x1f0 mm/kasan/report.c:450 mm/kasan/report.c:450 nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 __nf_register_net_hook+0x27e/0x8d0 net/netfilter/core.c:429 net/netfilter/core.c:429 nf_register_net_hook+0xaa/0x180 net/netfilter/core.c:571 net/netfilter/core.c:571 nft_register_flowtable_net_hooks+0x3c5/0x730 net/netfilter/nf_tables_api.c:7232		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/nf_tables_api.c:7232 nf_tables_newflowtable+0x2022/0x2cf0 net/netfilter/nf_tables_api.c:7430 net/netfilter/nf_tables_api.c:7430 nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv+0x10e6/0x2550 net/netfilter/nfnetlink.c:652 net/netfilter/nfnetlink.c:652		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__nft_release_hook( ) calls nft_unregister_flowtable_net_hooks() which only unregisters the hooks, then after RCU grace period, it is guaranteed that no packets add new entries to the flowtable (no flow offload rules and flowtable hooks are reachable from packet path), so it is safe to call nf_flow_table_free( ) which cleans up the remaining entries from the flowtable (both software and hardware) and it unbinds the flow_block. **CVE ID: CVE-2022-48935**		
Affected Version(s): * Up to (excluding) 4.19.320					
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk	https://git.kernel.org/stable/c/166a0bddcc27de41fe13f861c8348e8e53e988c8 , https://git.kernel.org/stable/c/47b3dce100778001cd76f7e9188944b5cb27a76	O-LIN-LINU-030924/1097

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QT	d, https://git.kernel.org/stable/c/7789a1d6792af410aa9b39a1eb237ed24fa2170a	

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9] dump_backtrace+0x0/0x1c0 [66.575469s] [pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s] [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42301		
Affected Version(s): * Up to (excluding) 4.9.305					
Double Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60	https://git.kernel.org/stable/c/147a0e71ccf96df9fc8c2ac500829d8e423ef02c, https://git.kernel.org/stable/c/2fe0e281f7ad0a62259649764228227dd6b2561d, https://git.kernel.org/stable/c/3d6cc9898efdfb062efb74dc18cfc700e082f5d5	O-LIN-LINU-030924/1098

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4 [Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ?		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0 [Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0 ... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ___kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+0x12/0x20		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae **CVE ID: CVE-2022-48919**		
Affected Version(s): * Up to (excluding) 5.10.103					
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: make apf token non-zero to fix bug In current async pagefault logic, when a page is ready, KVM relies on kvm_arch_can_dequeue_async_page_p	https://git.kernel.org/stable/c/4c3644b6c96c5daa5149e5abddc07234eea47c7c, https://git.kernel.org/stable/c/62040f5cd7d937de547836e747b6aa8212fec573, https://git.kernel.org/stable/c/6f3c1fc53d86d580d8d6d749c	O-LIN-LINU-030924/1099

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resent() to determine whether to deliver a READY event to the Guest. This function test token value of struct kvm_vcpu_pv_apf_data, which must be reset to zero by Guest kernel when a READY event is finished by Guest. If value is zero meaning that a READY event is done, so the KVM can deliver another. But the kvm_arch_setup_async_pf() may produce a valid token with zero value, which is confused with previous mention and may lead the loss of this READY event. This bug may cause task blocked forever in Guest: INFO: task stress:7532 blocked for more than 1254 seconds.	4af23705e4f6f79	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Not tainted 5.10.0 #16 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:stress state:D stack: 0 pid: 7532 ppid: 1409 flags:0x00000080 Call Trace: __schedule+0x1e7/0x650 schedule+0x46/0xb0 kvm_async_pf_task_wait_schedule+0xad/0xe0 ? exit_to_user_mode_prepare+0x60/0x70 __kvm_handle_async_pf+0x4f/0xb0 ? asm_exc_page_fault+0x8/0x30 exc_page_fault+0x6f/0x110 ? asm_exc_page_fault+0x8/0x30		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			asm_exc_page_fault+0x1e/0x30 RIP: 0033:0x402d00 RSP: 002b:00007ffd31912500 EFLAGS: 00010206 RAX: 0000000000071000 RBX: ffffffffffffffff RCX: 00000000021a32b0 RDX: 000000000007d011 RSI: 000000000007d000 RDI: 00000000021262b0 RBP: 00000000021262b0 R08: 0000000000000003 R09: 0000000000000086 R10: 00000000000000eb R11: 00007fefbdf2baa0 R12: 0000000000000000 R13: 0000000000000002 R14: 000000000007d000 R15:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000001000 **CVE ID: CVE-2022-48943**		
Integer Overflow or Wraparound	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: CDC-NCM: avoid overflow in sanity checking A broken device may give an extreme offset like 0xFFF0 and a reasonable length for a fragment. In the sanity check as formulated now, this will create an integer overflow, defeating the sanity check. Both offset and offset + len need to be checked in such a manner that no overflow can occur. And those quantities should be unsigned. **CVE ID: CVE-2022-48938**	https://git.kernel.org/stable/c/49909c9f8458cacb5b241106cba65aba5a6d8f4c, https://git.kernel.org/stable/c/69560efa001397ebb8dc1c3e6a3ce00302bb9f7f, https://git.kernel.org/stable/c/7b737e47b87589031f0d4657f6d7b0b770474925	O-LIN-LINU-030924/1100
Affected Version(s): * Up to (excluding) 5.10.104					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: ice: fix concurrent reset and removal of VFs Commit c503e63200c6 ("ice: Stop processing VF messages during teardown") introduced a driver state flag, ICE_VF_DEINIT_IN_PROGRESS, which is intended to prevent some issues with concurrently handling messages from VFs while tearing down the VFs. This change was motivated by crashes caused while tearing down and bringing up VFs in rapid succession. It turns out that the fix actually introduces issues with the VF driver	https://git.kernel.org/stable/c/05ae1f0fe9c6c5ead08b306e665763a352d20716, https://git.kernel.org/stable/c/2a3e61de89bab6696aa28b70030eb119968c5586, https://git.kernel.org/stable/c/3c805fce07c9dbc47d8a9129c7c5458025951957	O-LIN-LINU-030924/1101

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			caused because the PF no longer responds to any messages sent by the VF during its .remove routine. This results in the VF potentially removing its DMA memory before the PF has shut down the device queues. Additionally, the fix doesn't actually resolve concurrency issues within the ice driver. It is possible for a VF to initiate a reset just prior to the ice driver removing VFs. This can result in the remove task concurrently operating while the VF is being reset. This results in similar memory corruption and panics purportedly fixed by that commit. Fix this concurrency at its		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			root by protecting both the reset and removal flows using the existing VF cfg_lock. This ensures that we cannot remove the VF while any outstanding critical tasks such as a virtchnl message or a reset are occurring. This locking change also fixes the root cause originally fixed by commit c503e63200c6 ("ice: Stop processing VF messages during teardown"), so we can simply revert it. Note that I kept these two changes together because simply reverting the original commit alone would leave the driver vulnerable to worse race conditions. **CVE ID: CVE-2022-48941**		
Affected Version(s): * Up to (excluding) 5.10.224					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a DPC event occurs concurrently to hot-removal of the same portion of the hierarchy: The dpc_handler() awaits readiness of the secondary bus below the Downstream Port where the DPC event occurred. To do so, it polls the config space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct pci_dev cause the kernel to oops. That's because pci_bridge_wait_for	https://git.kernel.org/stable/c/11a1f4bc47362700fcbde717292158873fb847ed, https://git.kernel.org/stable/c/2c111413f38ca5cf87557cab89f6d82b0e3433e7, https://git.kernel.org/stable/c/2cc8973bdc4d6c928ebe38b88090a2cdfe81f42f	O-LIN-LINU-030924/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	_secondary_bus() neglects to hold a reference on the child device. Before v6.3, the function was only called on resume from system sleep or on runtime resume. Holding a reference wasn't necessary back then because the pciehp IRQ thread could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the resume_noirq phase. And runtime resume is always awaited before a PCI device is removed.) However starting with v6.3, pci_bridge_wait_for_secondary_bus() is also called on a DPC event. Commit 53b54ad074de ("PCI/DPC: Await readiness of secondary bus after reset"), which		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	introduced that, failed to appreciate that pci_bridge_wait_for _secondary_bus() now needs to hold a reference on the child device because dpc_handler() and pciehp may indeed run concurrently. The commit was backported to v5.10+ stable kernels, so that's the oldest one affected. Add the missing reference acquisition. Abridged stack trace: BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464 Comm: irq/53-pcie-dpc 6.9.0 RIP: pci_bus_read_config_dword+0x17/0x50		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			pci_dev_wait()
			pci_bridge_wait_for_secondary_bus()
			dpc_reset_link()
			pcie_do_recovery()
			dpc_handler()
			CVE ID: CVE-2024-42302		

NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference in apply_state_adjust_rules Check the pointer value to fix potential null pointer dereference **CVE ID: CVE-2024-43907**	https://git.kernel.org/stable/c/0c065e50445aea2e0a1815f12e97ee49e02cbaac, https://git.kernel.org/stable/c/13937a40aae4efe64592ba48c057ac3c72f7fe82, https://git.kernel.org/stable/c/3a01bf2ca9f860fdc88c358567b8fa3033efcf30	O-LIN-LINU-030924/1103
Affected Version(s): * Up to (excluding) 5.15.165					
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checker before passing variables	https://git.kernel.org/stable/c/1686675405d07f35eae7ff3d13a530034b899df2, https://git.kernel.org/stable/c/4cc2a94d96caeb3c975acdae73	O-LIN-LINU-030924/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Checks null pointer before passing variables to functions. This fixes 3 NULL_RETURNS issues reported by Coverity. **CVE ID: CVE-2024-43902**	51c2f997c32175, https://git.kernel.org/stable/c/8092aa3ab8f7b737a34b71f91492c676a843043a	
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference for smu7 optimize the code to avoid pass a null pointer (hwmgr->backend) to function smu7_update_edc_leakage_table. **CVE ID: CVE-2024-43909**	https://git.kernel.org/stable/c/09544cd95c688d3041328a4253bd7514972399bb, https://git.kernel.org/stable/c/1b8aa82b80bd947b68a8ab051d960a0c7935e22d, https://git.kernel.org/stable/c/37b9df457cbcf095963d18f17d6cb7dfa0a03fce	O-LIN-LINU-030924/1105
Affected Version(s): * Up to (excluding) 5.4.282					
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer	https://git.kernel.org/stable/c/033187a70ba9743c73a810a006816e5553d1e7d4, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1106

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference to ras_manager Check ras_manager before using it **CVE ID: CVE-2024-43908**	48cada0ac79e4775236d642e9ec5998a7c7fb7a4, https://git.kernel.org/stable/c/4c11d30c95576937c6c35e6f29884761f2dddb43	
Affected Version(s): * Up to (excluding) 6.1.103					
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md: fix deadlock between mddev_suspend and flush bio Deadlock occurs when mddev is being suspended while some flush bio is in progress. It is a complex issue. T1. the first flush is at the ending stage, it clears 'mddev->flush_bio' and tries to submit data, but is blocked because mddev is suspended by T4.	https://git.kernel.org/stable/c/2d0738a8322bf4e5bfe693d16b3111928a9ccfbf, https://git.kernel.org/stable/c/32226070813140234b6c507084738e8e8385c5c6, https://git.kernel.org/stable/c/611d5cbc0b35a752e657a83eebadf40d814d006b	O-LIN-LINU-030924/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			T2. the second flush sets 'mddev->flush_bio', and attempts to queue md_submit_flush_data(), which is already running (T1) and won't execute again if on the same CPU as T1. T3. the third flush inc active_io and tries to flush, but is blocked because 'mddev->flush_bio' is not NULL (set by T2). T4. mddev_suspend() is called and waits for active_io dec to 0 which is inc by T3. T1 T2 T3 T4 (flush 1) (flush 2) (third 3) (suspend) md_submit_flush_data mddev->flush_bio = NULL; .		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			. md_flush_request . mddev->flush_bio = bio . queue submit_flushes . . . . md_handle_request . . active_io + 1 . . md_flush_request . . wait !mddev->flush_bio . . . . mddev_suspend . . wait !active_io . . . submit_flushes . queue_work		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			md_submit_flush_data . //md_submit_flush_data is already running (T1) . md_handle_request wait resume The root issue is non-atomic inc/dec of active_io during flush process. active_io is dec before md_submit_flush_data is queued, and inc soon after md_submit_flush_data() run. md_flush_request active_io + 1 submit_flushes active_io - 1 md_submit_flush_data md_handle_request active_io + 1 make_request active_io - 1 If active_io is dec after		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			md_handle_request() instead of within submit_flushes(), make_request() can be called directly intead of md_handle_request() in md_submit_flush_data(), and active_io will only inc and dec once in the whole flush process. Deadlock will be fixed. Additionally, the only difference between fixing the issue and before is that there is no return error handling of make_request(). But after previous patch cleaned md_write_start(), make_requst() only return error in raid5_make_request() by dm-raid, see commit 41425f96d7aa ("dm-raid456, md/raid456: fix a deadlock for dm-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			raid456 while io concurrent with reshape)". Since dm always splits data and flush operation into two separate io, io size of flush submitted by dm always is 0, make_request() will not be called in md_submit_flush_data(). To prevent future modifications from introducing issues, add WARN_ON to ensure make_request() no error is returned in this context. **CVE ID: CVE-2024-43855**		
Affected Version(s): * Up to (excluding) 6.1.105					
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: xc2028: avoid use-after-free in load_firmware_cb() syzkaller reported use-after-free in load_firmware_cb() [1]. The reason is because the module	https://git.kernel.org/stable/c/208deb6d8c3cb8c3acb1f41eb31cf68ea08726d5, https://git.kernel.org/stable/c/68594cec291ff9523b9feb3f43fd853dcddd1f60, https://git.kernel.org/stable/c/850304152d367f104d21c77cfbcc05806504218b	O-LIN-LINU-030924/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated a struct tuner in tuner_probe(), and then the module initialization failed, the struct tuner was released. A worker which created during module initialization accesses this struct tuner later, it caused use-after-free. The process is as follows: task-6504 worker_thread tuner_probe <= alloc dvb_frontend [2] ... request_firmware_nowait <= create a worker ... tuner_remove <= free dvb_frontend ... request_firmware_work_func <= the firmware is ready		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			load_firmware_cb <= but now the dvb_frontend has been freed To fix the issue, check the dvd_frontend in load_firmware_cb(), if it is null, report a warning and just return. [1]: == BUG: KASAN: use-after-free in load_firmware_cb+0x1310/0x17a0 Read of size 8 at addr ffff8000d7ca2308 by task kworker/2:3/6504 Call trace: load_firmware_cb+0x1310/0x17a0 request_firmware_work_func+0x128/0x220		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	process_one_work+0x770/0x1824 worker_thread+0x488/0xea0 kthread+0x300/0x430 ret_from_fork+0x10/0x20 Allocated by task 6504: kzalloc tuner_probe+0xb0/0x1430 i2c_device_probe+0x92c/0xaf0 really_probe+0x678/0xcd0 driver_probe_device+0x280/0x370 __device_attach_driver+0x220/0x330 bus_for_each_drv+0x134/0x1c0 __device_attach+0x1f4/0x410		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	device_initial_probe+0x20/0x30 bus_probe_device+0x184/0x200 device_add+0x924/0x12c0 device_register+0x24/0x30 i2c_new_device+0x4e0/0xc44 v4l2_i2c_new_subdev_board+0xbc/0x290 v4l2_i2c_new_subdev+0xc8/0x104 em28xx_v4l2_init+0x1dd0/0x3770 Freed by task 6504: kfree+0x238/0x4e4 tuner_remove+0x144/0x1c0 i2c_device_remove+0xc8/0x290		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__device_release_driver+0x314/0x5fc device_release_driver+0x30/0x44 bus_remove_device+0x244/0x490 device_del+0x350/0x900 device_unregister+0x28/0xd0 i2c_unregister_device+0x174/0x1d0 v4l2_device_unregister+0x224/0x380 em28xx_v4l2_init+0x1d90/0x3770 The buggy address belongs to the object at ffff8000d7ca2000 which belongs to the cache kmalloc-2k of size 2048 The buggy address is located 776 bytes inside of 2048-byte region [ffff8000d7ca2000, ffff8000d7ca2800)		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	The buggy address belongs to the page: page:ffff7fe00035f280 count:1 mapcount:0 mapping:ffff8000c001f000 index:0x0 flags: 0x7ff800000000100(slab) raw: 07ff800000000100 ffff7fe00049d880 0000000300000003 ffff8000c001f000 raw: 0000000000000000 0000000080100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff8000d7ca2200: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2280: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff8000d7ca2300		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff8000d7ca2380: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2400: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == [2] Actually, it is allocated for struct tuner, and dvb_frontend is inside. **CVE ID: CVE-2024-43900**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add NULL check for 'afb' before dereferencing in amdgpu_dm_plane_handle_cursor_update	https://git.kernel.org/stable/c/31a679a880102dee6e10985a7b1789af8dc328cc, https://git.kernel.org/stable/c/38e6f715b02b572f74677eb2f29d3b4bc6f1ddff, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1109

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This commit adds a null check for the 'afb' variable in the amdgpu_dm_plane_handle_cursor_update function. Previously, 'afb' was assumed to be null, but was used later in the code without a null check. This could potentially lead to a null pointer dereference. Fixes the below: drivers/gpu/drm/amd/amdgpu/../display/amdgpu_dm/amdgpu_dm_plane.c:1298 amdgpu_dm_plane_handle_cursor_update() error: we previously assumed 'afb' could be null (see line 1252) **CVE ID: CVE-2024-43903**	94220b35aeba2b68da81deeefbb784d94eeb5c04	
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix the null pointer	https://git.kernel.org/stable/c/2e538944996d0dd497faf8ee81f8bfcd3aca7d80, https://git.kernel.org/stable/c/50151b7f1c79a	O-LIN-LINU-030924/1110

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference for vega10_hwmgr Check return value and conduct null pointer handling to avoid null pointer dereference. **CVE ID: CVE-2024-43905**	09117837eb95b76c2de76841dab, https://git.kernel.org/stable/c/69a441473fec2fc2aa2cf56122d6c42c4266a239	
Affected Version(s): * Up to (excluding) 6.10.5					
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null check in resource_log_pipe_topology_update [WHY] When switching from "Extend" to "Second Display Only" we sometimes call resource_get_otg_master_for_stream on a stream for the eDP, which is disconnected. This leads to a null pointer dereference. [HOW]	https://git.kernel.org/stable/c/899d92fd26fe780aad711322aa671f68058207a6, https://git.kernel.org/stable/c/c36e922a36bdf69765c340a0857ca74092003bee	O-LIN-LINU-030924/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Added a null check in dc_resource.c/resource_log_pipe_topology_update. **CVE ID: CVE-2024-43886**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix null pointer deref in dcn20_resource.c Fixes a hang thats triggered when MPV is run on a DCN401 dGPU: mpv --hwdec=vaapi --vo=gpu --hwdec-codecs=all and then enabling fullscreen playback (double click on the video) The following calltrace will be seen: [181.843989] BUG: kernel NULL pointer	https://git.kernel.org/stable/c/974fccd61758599a9716c4b909d9226749efe37e, https://git.kernel.org/stable/c/ecbf60782662f0a388493685b85a645a0ba1613c	O-LIN-LINU-030924/1112

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference, address: 0000000000000000 [181.843997] #PF: supervisor instruction fetch in kernel mode [181.844003] #PF: error_code(0x0010) - not-present page [181.844009] PGD 0 P4D 0 [181.844020] Oops: 0010 [#1] PREEMPT SMP NOPTI [181.844028] CPU: 6 PID: 1892 Comm: gnome-shell Tainted: G W OE 6.5.0-41-generic #41~22.04.2-Ubuntu [181.844038] Hardware name: System manufacturer System Product Name/CROSSHAIR VI HERO, BIOS 6302 10/23/2018 [181.844044] RIP: 0010:0x0 [181.844079] Code: Unable to access opcode bytes at 0xffffffffffffffd6.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[181.844084] RSP: 0018:ffffb593c2b8f7b0 EFLAGS: 00010246 [181.844093] RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000004 [181.844099] RDX: ffffb593c2b8f804 RSI: ffffb593c2b8f7e0 RDI: ffff9e3c8e758400 [181.844105] RBP: ffffb593c2b8f7b8 R08: ffffb593c2b8f9c8 R09: ffffb593c2b8f96c [181.844110] R10: 0000000000000000 R11: 0000000000000000 R12: ffffb593c2b8f9c8 [181.844115] R13: 0000000000000001 R14: ffff9e3c88000000 R15: 0000000000000005 [181.844121] FS: 00007c6e323bb5c0(0000)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GS:ffff9e3f85f80000(0000) knlGS:0000000000000000 [181.844128] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [181.844134] CR2: ffffffffffffffd6 CR3: 0000000140fbe000 CR4: 00000000003506e0 [181.844141] Call Trace: [181.844146] <TASK> [181.844153] ? show_regs+0x6d/0x80 [181.844167] ? __die+0x24/0x80 [181.844179] ? page_fault_oops+0x99/0x1b0 [181.844192] ? do_user_addr_fault+0x31d/0x6b0 [181.844204] ? exc_page_fault+0x83/0x1b0 [181.844216] ? asm_exc_page_fault+0x27/0x30 [181.844237] dcn20_get_dcc_compression_cap+0x23/0x30 [amdgpu]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[181.845115] amdgpu_dm_plane_validate_dcc.constprop.0+0xe5/0x180 [amdgpu] [181.845985] amdgpu_dm_plane_fill_plane_buffer_attributes+0x300/0x580 [amdgpu] [181.846848] fill_dc_plane_info_and_addr+0x258/0x350 [amdgpu] [181.847734] fill_dc_plane_attributes+0x162/0x350 [amdgpu] [181.848748] dm_update_plane_state.constprop.0+0x4e3/0x6b0 [amdgpu] [181.849791] ? dm_update_plane_state.constprop.0+0x4e3/0x6b0 [amdgpu] [181.850840] amdgpu_dm_atomic_check+0xdfe/0x1760 [amdgpu] **CVE ID: CVE-2024-43899**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix NULL pointer	https://git.kernel.org/stable/c/1e68b7ce6bc6073579fe8713ec6b85aa9cd2e351, https://git.kern	O-LIN-LINU-030924/1113

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	dereference for DTN log in DCN401 When users run the command: cat /sys/kernel/debug/dri/0/amdgpu_dm_dtn_log The following NULL pointer dereference happens: [+0.000003] BUG: kernel NULL pointer dereference, address: NULL [+0.000005] #PF: supervisor instruction fetch in kernel mode [+0.000002] #PF: error_code(0x0010) - not-present page [+0.000002] PGD 0 P4D 0 [+0.000004] Oops: 0010 [#1] PREEMPT SMP NOPTI [+0.000003] RIP: 0010:0x0 [+0.000008] Code: Unable to access	el.org/stable/c/5af757124792817f8eb1bd0c80ad60fab519586b	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			opcode bytes at 0xffffffffffffffd6. [...] [+0.000002] PKRU: 55555554 [+0.000002] Call Trace: [+0.000002] <TASK> [+0.000003] ? show_regs+0x65/0x70 [+0.000006] ? __die+0x24/0x70 [+0.000004] ? page_fault_oops+0x160/0x470 [+0.000006] ? do_user_addr_fault+0x2b5/0x690 [+0.000003] ? prb_read_valid+0x1c/0x30 [+0.000005] ? exc_page_fault+0x8c/0x1a0 [+0.000005] ? asm_exc_page_fault+0x27/0x30 [+0.000012] dcn10_log_color_state+0xf9/0x510 [amdgpu] [+0.000306] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000003] ? vsnprintf+0x2fb/0x600		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[+0.000009] dcn10_log_hw_state+0xfd0/0xfe0 [amdgpu] [+0.000218] ? __mod_memcg_lruvec_state+0xe8/0x170 [+0.000008] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? debug_smp_processor_id+0x17/0x20 [+0.000003] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? set_ptes.isra.0+0x2b/0x90 [+0.000004] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? _raw_spin_unlock+0x19/0x40 [+0.000004] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? do_anonymous_page+0x337/0x700 [+0.000004] dtn_log_read+0x82/0x120 [amdgpu]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[+0.000207] full_proxy_read+0x66/0x90 [+0.000007] vfs_read+0xb0/0x340 [+0.000005] ? __count_memcg_events+0x79/0xe0 [+0.000002] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000003] ? count_memcg_events.constprop.0+0x1e/0x40 [+0.000003] ? handle_mm_fault+0xb2/0x370 [+0.000003] ksys_read+0x6b/0xf0 [+0.000004] __x64_sys_read+0x19/0x20 [+0.000003] do_syscall_64+0x60/0x130 [+0.000004] entry_SYSCALL_64_after_hwframe+0x6e/0x76 [+0.000003] RIP: 0033:0x7fdf32f147e2 [...] This error happens when the color log		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tries to read the gamut remap information from DCN401 which is not initialized in the dcn401_dpp_funcs which leads to a null pointer dereference. This commit addresses this issue by adding a proper guard to access the gamut_remap callback in case the specific ASIC did not implement this function. **CVE ID: CVE-2024-43901**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checks for 'stream' and 'plane' before dereferencing This commit adds null checks for the 'stream' and 'plane' variables in the dcn30_apply_idle_p	https://git.kernel.org/stable/c/15c2990e0f0108b9c3752d7072a97d45d4283aea, https://git.kernel.org/stable/c/16a8a2a839d19c4cf7253642b493ffb8eee1d857	O-LIN-LINU-030924/1114

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ower_optimizations function. These variables were previously assumed to be null at line 922, but they were used later in the code without checking if they were null. This could potentially lead to a null pointer dereference, which would cause a crash. The null checks ensure that 'stream' and 'plane' are not null before they are used, preventing potential crashes. Fixes the below static smatch checker: drivers/gpu/drm/amd/amdgpu/../display/dc/hwss/dcn30/dcn30_hwseq.c:938 dcn30_apply_idle_power_optimizations() error: we previously assumed 'stream' could be null (see line 922)		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/gpu/drm/amd/amdgpu/../display/dc/hwss/dcn30/dcn30_hwseq.c:940 dcn30_apply_idle_power_optimizations() error: we previously assumed 'plane' could be null (see line 922) **CVE ID: CVE-2024-43904**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix NULL dereference at band check in starting tx ba session In MLD connection, link_data/link_conf are dynamically allocated. They don't point to vif->bss_conf. So, there will be no chanreq assigned to vif->bss_conf and then the chan will be NULL. Tweak the code to check ht_supported/vht_supported/has_he/has_eht on sta deflink.	https://git.kernel.org/stable/c/021d53a3d87eeb9dbba524ac515651242a2a7e3b, https://git.kernel.org/stable/c/a5594c1e03b0df3908b1e1202a1ba34422eed0f6	O-LIN-LINU-030924/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Crash log (with rtw89 version under MLO development): [9890.526087] BUG: kernel NULL pointer dereference, address: 0000000000000000 [9890.526102] #PF: supervisor read access in kernel mode [9890.526105] #PF: error_code(0x0000) - not-present page [9890.526109] PGD 0 P4D 0 [9890.526114] Oops: 0000 [#1] PREEMPT SMP PTI [9890.526119] CPU: 2 PID: 6367 Comm: kworker/u16:2 Kdump: loaded Tainted: G OE 6.9.0 #1 [9890.526123] Hardware name: LENOVO 2356AD1/2356AD1, BIOS G7ETB3WW (2.73) 11/28/2018 [9890.526126] Workqueue: phy2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rtw89_core_ba_work [rtw89_core] [9890.526203] RIP: 0010:ieee80211_start_tx_ba_session (net/mac80211/agg-tx.c:618 (discriminator 1)) mac80211 [9890.526279] Code: f7 e8 d5 93 3e ea 48 83 c4 28 89 d8 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc 49 8b 84 24 e0 f1 ff ff 48 8b 80 90 1b 00 00 <83> 38 03 0f 84 37 fe ff ff bb ea ff ff ff eb cc 49 8b 84 24 10 f3 All code ======== 0: f7 e8 imul %eax 2: d5 (bad) 3: 93 xchg %eax,%ebx 4: 3e ea ds (bad) 6: 48 83 c4 28 add $0x28,%rsp a: 89 d8 mov %ebx,%eax c: 5b pop %rbx		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d: 41 5c pop %r12 f: 41 5d pop %r13 11: 41 5e pop %r14 13: 41 5f pop %r15 15: 5d pop %rbp 16: c3 retq 17: cc int3 18: cc int3 19: cc int3 1a: cc int3 1b: 49 8b 84 24 e0 f1 ff mov -0xe20(%r12),%rax 22: ff 23: 48 8b 80 90 1b 00 00 mov 0x1b90(%rax),%rax 2a:* 83 38 03 cmpl $0x3,(%rax) <-- trapping instruction 2d: 0f 84 37 fe ff ff je 0xfffffffffffffe6a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			33: bb ea ff ff ff mov $0xffffffea,%ebx 38: eb cc jmp 0x6 3a: 49 rex.WB 3b: 8b .byte 0x8b 3c: 84 24 10 test %ah,(%rax,%rdx,1) 3f: f3 repz Code starting with the faulting instruction === 0: 83 38 03 cmpl $0x3,(%rax) 3: 0f 84 37 fe ff ff je 0xfffffffffffffe40 9: bb ea ff ff ff mov $0xffffffea,%ebx e: eb cc jmp 0xffffffffffffffdc 10: 49 rex.WB 11: 8b .byte 0x8b		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12: 84 24 10 test %ah,(%rax,%rdx,1) 15: f3 repz [9890.526285] RSP: 0018:ffffb8db09013d68 EFLAGS: 00010246 [9890.526291] RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff9308e0d656c8 [9890.526295] RDX: 0000000000000000 RSI: ffffffffab99460b RDI: ffffffffab9a7685 [9890.526300] RBP: ffffb8db09013db8 R08: 0000000000000000 R09: 0000000000000873 [9890.526304] R10: ffff9308e0d64800 R11: 0000000000000002 R12: ffff9308e5ff6e70 [9890.526308] R13:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff930952500e20 R14: ffff9309192a8c00 R15: 0000000000000000 [9890.526313] FS: 0000000000000000(0000) GS:ffff930b4e700000(0000) knlGS:0000000000000000 [9890.526316] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [9890.526318] CR2: 0000000000000000 CR3: 0000000391c58005 CR4: 00000000001706f0 [9890.526321] Call Trace: [9890.526324] <TASK> [9890.526327] ? show_regs (arch/x86/kernel/dumpstack.c:479) [9890.526335] ? __die (arch/x86/kernel/dumpstack.c:421 arch/x86/kernel/dumpstack.c:434)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[9890.526340] ? page_fault_oops (arch/x86/mm/fault.c:713) [9890.526347] ? search_module_extables (kernel/module/main.c:3256 (discriminator ---truncated--- **CVE ID: CVE-2024-43911**		
Affected Version(s): * Up to (excluding) 6.6.46					
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/admgpu: fix dereferencing null pointer context When user space sets an invalid ta type, the pointer context will be empty. So it need to check the pointer context before using it **CVE ID: CVE-2024-43906**	https://git.kernel.org/stable/c/030ffd4d43b433bc6671d9ec34fc12c59220b95d, https://git.kernel.org/stable/c/4fd52f7c2c11d330571c6bde06e5ea508ec25c9d, https://git.kernel.org/stable/c/641dac64178ccdb9e45c92b67120316896294d05	O-LIN-LINU-030924/1116
Affected Version(s): * Up to (excluding) 6.6.47					
N/A	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/26c07775fb5dc74351d1c3a2bc3cdf609b03e49f,	O-LIN-LINU-030924/1117

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	f2fs: fix to do sanity check on F2FS_INLINE_DATA flag in inode during GC syzbot reports a f2fs bug as below: ------------[cut here]------------ kernel BUG at fs/f2fs/inline.c:258! CPU: 1 PID: 34 Comm: kworker/u8:2 Not tainted 6.9.0-rc6-syzkaller-00012-g9e4bc4bcae01 #0 RIP: 0010:f2fs_write_inline_data+0x781/0x790 fs/f2fs/inline.c:258 Call Trace: f2fs_write_single_data_page+0xb65/0x1d60 fs/f2fs/data.c:2834 f2fs_write_cache_pages fs/f2fs/data.c:3133 [inline] __f2fs_write_data_pages	https://git.kernel.org/stable/c/ae00e6536a2dd54b64b39e9a39548870cf835745, https://git.kernel.org/stable/c/fc01008c92f40015aeeced94750855a7111b6929	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fs/f2fs/data.c:3288 [inline] f2fs_write_data_pages+0x1efe/0x3a90 fs/f2fs/data.c:3315 do_writepages+0x35b/0x870 mm/page-writeback.c:2612 __writeback_single_inode+0x165/0x10b0 fs/fs-writeback.c:1650 writeback_sb_inodes+0x905/0x1260 fs/fs-writeback.c:1941 wb_writeback+0x457/0xce0 fs/fs-writeback.c:2117 wb_do_writeback fs/fs-writeback.c:2264 [inline] wb_workfn+0x410/0x1090 fs/fs-writeback.c:2304 process_one_work kernel/workqueue.c:3254 [inline] process_scheduled_works+0xa12/0x17c0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel/workqueue.c:3335 worker_thread+0x86d/0xd70 kernel/workqueue.c:3416 kthread+0x2f2/0x390 kernel/kthread.c:388 ret_from_fork+0x4d/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244 The root cause is: inline_data inode can be fuzzed, so that there may be valid blkaddr in its direct node, once f2fs triggers background GC to migrate the block, it will hit f2fs_bug_on() during dirty page writeback. Let's add sanity check on F2FS_INLINE_DAT		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A flag in inode during GC, so that, it can forbid migrating inline_data inode's data block for fixing. **CVE ID: CVE-2024-44942**		
Affected Version(s): 6.10.4					
Out-of-bounds Write	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bnxt_en : Fix memory out-of-bounds in bnxt_fill_hw_rss_tbl() A recent commit has modified the code in __bnxt_reserve_rings() to set the default RSS indirection table to default only when the number of RX rings is changing. While this works for newer firmware that requires RX ring reservations, it causes the regression on older	https://git.kernel.org/stable/c/abd573e9ad2ba64eaa6418a5f4eec819de28f205, https://git.kernel.org/stable/c/da03f5d1b2c319a2b74fe76edeadcd8fa5f44376	O-LIN-LINU-030924/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware not requiring RX ring resrvations (BNXT_NEW_RM() returns false). With older firmware, RX ring reservations are not required and so hw_resc->resv_rx_rings is not always set to the proper value. The comparison: if (old_rx_rings != bp->hw_resc.resv_rx_rings) in __bnxt_reserve_rings() may be false even when the RX rings are changing. This will cause __bnxt_reserve_rings() to skip setting the default RSS indirection table to default to match the current number of RX rings. This may later cause		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bnxt_fill_hw_rss_tbl() to use an out-of-range index. We already have bnxt_check_rss_tbl_no_rmgr() to handle exactly this scenario. We just need to move it up in bnxt_need_reserve_rings() to be called unconditionally when using older firmware. Without the fix, if the TX rings are changing, we'll skip the bnxt_check_rss_tbl_no_rmgr() call and __bnxt_reserve_rings() may also skip the bnxt_set_dflt_rss_indir_tbl() call for the reason explained in the last paragraph. Without setting the default RSS indirection table to default, it causes the regression:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KASAN: slab-out-of-bounds in __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 Read of size 2 at addr ffff8881c5809618 by task ethtool/31525 Call Trace: __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 bnxt_hwrm_vnic_rss_cfg_p5+0xf7/0x460 __bnxt_setup_vnic_p5+0x12e/0x270 __bnxt_open_nic+0x2262/0x2f30 bnxt_open_nic+0x5d/0xf0 ethnl_set_channels+0x5d4/0xb30 ethnl_default_set_doit+0x2f1/0x620 **CVE ID: CVE-2024-44933**		
Affected Version(s): 6.11					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98	O-LIN-LINU-030924/1119

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03	d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding handling is missing.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv. **CVE ID: CVE-2024-42271**		
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: mm: list_lru: fix UAF for memory cgroup The mem_cgroup_from_slab_obj() is supposed to be called under rcu lock or cgroup_mutex or others which could prevent returned memcg from being	https://git.kernel.org/stable/c/4589f77c18dd98b65f45617b6d1e95313cf6fcab , https://git.kernel.org/stable/c/5161b48712dcd08ec427c450399d4d1483e21dea	O-LIN-LINU-030924/1120

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			freed. Fix it by adding missing rcu read lock. Found by code inspection. [songmuchun@bytedance.com: only grab rcu lock when necessary, per Vlastimil] Link: https://lkml.kernel.org/r/20240801024603.1865-1-songmuchun@bytedance.com **CVE ID: CVE-2024-43888**		
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: idpf: fix UAFs when destroying the queues The second tagged commit started sometimes (very rarely, but possible) throwing WARNs from net/core/page_pool.c:page_pool_disab	https://git.kernel.org/stable/c/290f1c033281c1a502a3cd1c53c3a549259c491f, https://git.kernel.org/stable/c/3cde714b0e77206ed1b5cf31f28c18ba9ae946fd	O-LIN-LINU-030924/1121

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			le_direct_recycling( ). Turned out idpf frees interrupt vectors with embedded NAPIs *before* freeing the queues making page_pools' NAPI pointers lead to freed memory before these pools are destroyed by libeth. It's not clear whether there are other accesses to the freed vectors when destroying the queues, but anyway, we usually free queue/interrupt vectors only when the queues are destroyed and the NAPIs are guaranteed to not be referenced anywhere. Invert the allocation and freeing logic making queue/interrupt vectors be allocated first and freed last. Vectors don't		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require queues to be present, so this is safe. Additionally, this change allows to remove that useless queue->q_vector pointer cleanup, as vectors are still valid when freeing the queues (+ both are freed within one function, so it's not clear why nullify the pointers at all). **CVE ID: CVE-2024-44932**		
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: wait for previous gc cycles when removing port syzbot hit a use-after-free[1] which is caused because the bridge doesn't make sure that all previous garbage has been collected when removing a port. What happens is:	https://git.kernel.org/stable/c/0d8b26e10e680c01522d7cc14abe04c3265a928f, https://git.kernel.org/stable/c/1e16828020c674b3be85f52685e8b80f9008f50f, https://git.kernel.org/stable/c/92c4ee25208d0f35dafc3213cdf355fbe449e078	O-LIN-LINU-030924/1122

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU 1 CPU 2 start gc cycle remove port acquire gc lock first wait for lock call br_multicasg_gc() directly acquire lock now but free port the port can be freed while grp timers still running Make sure all previous gc cycles have finished by using flush_work before freeing the port. [1] BUG: KASAN: slab-use-after-free in br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 Read of size 8 at addr ffff888071d6d000 by task syz.5.1232/9699		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	CPU: 1 PID: 9699 Comm: syz.5.1232 Not tainted 6.10.0-rc5-syzkaller-00021-g24ca36a562d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 br_multicast_port_g		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			roup_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 call_timer_fn+0x1a3/0x610 kernel/time/timer.c:1792 expire_timers kernel/time/timer.c:1843 [inline] __run_timers+0x74b/0xaf0 kernel/time/timer.c:2417 __run_timer_base kernel/time/timer.c:2428 [inline] __run_timer_base kernel/time/timer.c:2421 [inline] run_timer_base+0x111/0x190 kernel/time/timer.c:2437 **CVE ID: CVE-2024-44934**		
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the performance extension	https://git.kernel.org/stable/c/32df4abc44f24dbec239d43e2b26d5768c5d1a78, https://git.kernel.org/stable/c/ad5fdc48f7a63b8a98493c6675	O-LIN-LINU-030924/1123

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If fetching of userspace memory fails during the main loop, all drm sync objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from commit 484de39fa5f5b7bd0c5f2e2c5265167250ef7501) **CVE ID: CVE-2024-42262**	05fe4d3864ae21	
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the timestamp extension If fetching of userspace memory fails during the	https://git.kernel.org/stable/c/0e50fcc20bd87584840266e8004f9064a8985b4f, https://git.kernel.org/stable/c/9b5033ee2c5af6d1135a403df32d219ab57e55f9	O-LIN-LINU-030924/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			main loop, all drm sync objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from commit 753ce4fea62182c77e1691ab4f9022008f25b62e) **CVE ID: CVE-2024-42263**		
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix missing lock on sync reset reload On sync reset reload work, when remote host updates devlink on reload actions performed on that host, it misses taking devlink lock before	https://git.kernel.org/stable/c/091268f3c27a5b6d7858a3bb2a0dbcc9cd26ddb5, https://git.kernel.org/stable/c/572f9caa9e7295f8c8822e4122c7ae8f1c412ff9, https://git.kernel.org/stable/c/5d07d1d40aabfd61bab21115639bd4f641db6002	O-LIN-LINU-030924/1125

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling devlink_remote_reload_actions_performed() which results in triggering lock assert like the following: WARNING: CPU: 4 PID: 1164 at net/devlink/core.c: 261 devl_assert_locked +0x3e/0x50 ... CPU: 4 PID: 1164 Comm: kworker/u96:6 Tainted: G S W 6.10.0-rc2+ #116 Hardware name: Supermicro SYS-2028TP-DECTR/X10DRT-PT, BIOS 2.0 12/18/2015 Workqueue: mlx5_fw_reset_events mlx5_sync_reset_reload_work [mlx5_core] RIP: 0010:devl_assert_locked+0x3e/0x50 ... Call Trace: <TASK>		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	? __warn+0xa4/0x210 ? devl_assert_locked+0x3e/0x50 ? report_bug+0x160/0x280 ? handle_bug+0x3f/0x80 ? exc_invalid_op+0x17/0x40 ? asm_exc_invalid_op+0x1a/0x20 ? devl_assert_locked+0x3e/0x50 devlink_notify+0x88/0x2b0 ? mlx5_attach_device+0x20c/0x230 [mlx5_core] ? __pfx_devlink_notify+0x10/0x10 ? process_one_work+0x4b6/0xbb0 process_one_work+0x4b6/0xbb0 […]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42268		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix potential null-ptr-deref in ip6table_nat_table_init(). ip6table_nat_table_init() accesses net->gen->ptr[ip6table_nat_net_ops.id], but the function is exposed to user space before the entry is allocated via register_pernet_subsys(). Let's call register_pernet_subsys() before xt_register_template(). **CVE ID: CVE-2024-42269**	https://git.kernel.org/stable/c/419ee6274c5153b89c4393c1946faa4c3cad4f9e, https://git.kernel.org/stable/c/87dba44e9471b79b255d0736858a897332db9226, https://git.kernel.org/stable/c/91b6df6611b7edb28676c4f63f90c56c30d3e601	O-LIN-LINU-030924/1126
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix null-ptr-deref in	https://git.kernel.org/stable/c/08ed888b69a22647153fe2bec55b7cd0a46102cc, https://git.kern	O-LIN-LINU-030924/1127

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iptable_nat_table_init(). We had a report that iptables-restore sometimes triggered null-ptr-deref at boot time. [0] The problem is that iptable_nat_table_init() is exposed to user space before the kernel fully initialises netns. In the small race window, a user could call iptable_nat_table_init() that accesses net_generic(net, iptable_nat_net_id), which is available only after registering iptable_nat_net_ops. Let's call register_pernet_subsys() before xt_register_template(). [0]:	el.org/stable/c/5830aa863981d43560748aa93589c0695191d95d, https://git.kernel.org/stable/c/70014b73d7539fcbb6b4ff5f37368d7241d8e626	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	bpfilter: Loaded bpfilter_umh pid 11702 Started bpfilter BUG: kernel NULL pointer dereference, address: 0000000000000013 PF: supervisor write access in kernel mode PF: error_code(0x0002) - not-present page PGD 0 P4D 0 PREEMPT SMP NOPTI CPU: 2 PID: 11879 Comm: iptables-restor Not tainted 6.1.92-99.174.amzn2023.x86_64 #1 Hardware name: Amazon EC2 c6i.4xlarge/, BIOS 1.0 10/16/2017 RIP: 0010:iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat Code: 10 4c 89 f6 48 89 ef e8 0b 19 bb ff 41 89 c4 85 c0 75 38 41 83 c7 01 49		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			83 c6 28 41 83 ff 04 75 dc 48 8b 44 24 08 48 8b 0c 24 <48> 89 08 4c 89 ef e8 a2 3b a2 cf 48 83 c4 10 44 89 e0 5b 5d 41 5c RSP: 0018:ffffbef902843cd0 EFLAGS: 00010246 RAX: 0000000000000013 RBX: ffff9f4b052caa20 RCX: ffff9f4b20988d80 RDX: 0000000000000000 RSI: 0000000000000064 RDI: ffffffffc04201c0 RBP: ffff9f4b29394000 R08: ffff9f4b07f77258 R09: ffff9f4b07f77240 R10: 0000000000000000 R11: ffff9f4b09635388 R12: 0000000000000000 R13: ffff9f4b1a3c6c00 R14: ffff9f4b20988e20 R15:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000004 FS: 00007f6284340000(0000) GS:ffff9f51fe280000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000013 CR3: 00000001d10a6005 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259)		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? xt_find_table_lock (net/netfilter/x_tables.c:1259) ? __die_body.cold (arch/x86/kernel/dumpstack.c:478 arch/x86/kernel/dumpstack.c:420) ? page_fault_oops (arch/x86/mm/fault.c:727) ? exc_page_fault (./arch/x86/include/asm/irqflags.h:40 ./arch/x86/include/asm/irqflags.h:75 arch/x86/mm/fault.c:1470 arch/x86/mm/fault.c:1518) ? asm_exc_page_fault (./arch/x86/include/asm/idtentry.h:570) ? iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat xt_find_table_lock (net/netfilter/x_tables.c:1259)		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xt_request_find_table_lock (net/netfilter/x_tables.c:1287) get_info (net/ipv4/netfilter/ip_tables.c:965) ? security_capable (security/security.c:809 (discriminator 13)) ? ns_capable (kernel/capability.c:376 kernel/capability.c:397) ? do_ipt_get_ctl (net/ipv4/netfilter/ip_tables.c:1656) ? bpfilter_send_req (net/bpfilter/bpfilter_kern.c:52) bpfilter nf_getsockopt (net/netfilter/nf_sockopt.c:116) ip_getsockopt (net/ipv4/ip_sockglue.c:1827) __sys_getsockopt (net/socket.c:2327) __x64_sys_getsockopt (net/socket.c:2342 net/socket.c:2339 net/socket.c:2339) do_syscall_64 (arch/x86/entry/c		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ommon.c:51 arch/x86/entry/common.c:81) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) RIP: 0033:0x7f62844685ee Code: 48 8b 0d 45 28 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 37 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 0a c3 66 0f 1f 84 00 00 00 00 00 48 8b 15 09 RSP: 002b:00007ffd1f83d638 EFLAGS: 00000246 ORIG_RAX: 0000000000000037 RAX: ffffffffffffffda RBX: 00007ffd1f83d680 RCX: 00007f62844685ee RDX: 0000000000000040 RSI: 0000000000000000 RDI: 0000000000000004		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: 0000000000000004 R08: 00007ffd1f83d670 R09: 0000558798ffa2a0 R10: 00007ffd1f83d680 R11: 0000000000000246 R12: 00007ffd1f83e3b2 R13: 00007f6284 ---truncated--- **CVE ID: CVE-2024-42270**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Add error handling to pair_device() hci_conn_params_add() never checks for a NULL value and could lead to a NULL pointer dereference causing a crash. Fixed by adding error handling in the function. **CVE ID: CVE-2024-43884**	https://git.kernel.org/stable/c/538fd3921afac97158d4177139a0ad39f056dbb2	O-LIN-LINU-030924/1128

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double inode unlock for direct IO sync writes If we do a direct IO sync write, at btrfs_sync_file(), and we need to skip inode logging or we get an error starting a transaction or an error when flushing delalloc, we end up unlocking the inode when we shouldn't under the 'out_release_extents' label, and then unlock it again at btrfs_direct_write(). Fix that by checking if we have to skip inode unlocking under that label. **CVE ID: CVE-2024-43885**	https://git.kernel.org/stable/c/1a607d22dea4f60438747705495ec4d0af2ec451, https://git.kernel.org/stable/c/7ba27f14161fc20c4fc0051658a22ddd832eb0aa, https://git.kernel.org/stable/c/8bd4c9220416111500c275546c69c63d42185793	O-LIN-LINU-030924/1129
Divide By Zero	26-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/6d45e1c948a8b	O-LIN-LINU-030924/1130

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time. [10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1 [10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021 [10.017908] Workqueue: events_unbound padata_mt_helper	7ed6ceddb14319af69424db730c, https://git.kernel.org/stable/c/8f5ffd2af7274853ff91d6cd62541191d9fbd10d, https://git.kernel.org/stable/c/924f788c906dccaca30acab86c7124371e1d6f2c	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 : [10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330 [10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30 [10.018147] </TASK> Looking at the padata_mt_helper() function, the only way a divide-by-0 panic can happen is when ps->chunk_size is 0. The way that chunk_size is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least 1 no matter what the input parameters are. **CVE ID: CVE-2024-43889**		
Out-of-bounds Write	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bnxt_en : Fix memory out-of-bounds in bnxt_fill_hw_rss_tbl() A recent commit has modified the code in __bnxt_reserve_rings() to set the default RSS indirection table to default only when the number	https://git.kernel.org/stable/c/abd573e9ad2ba64eaa6418a5f4eec819de28f205, https://git.kernel.org/stable/c/da03f5d1b2c319a2b74fe76edeadcd8fa5f44376	O-LIN-LINU-030924/1131

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of RX rings is changing. While this works for newer firmware that requires RX ring reservations, it causes the regression on older firmware not requiring RX ring resrvations (BNXT_NEW_RM() returns false). With older firmware, RX ring reservations are not required and so hw_resc->resv_rx_rings is not always set to the proper value. The comparison: if (old_rx_rings != bp->hw_resc.resv_rx_rings) in __bnxt_reserve_rings() may be false even when the RX rings are changing. This will cause		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	__bnxt_reserve_rings() to skip setting the default RSS indirection table to default to match the current number of RX rings. This may later cause bnxt_fill_hw_rss_tbl() to use an out-of-range index. We already have bnxt_check_rss_tbl_no_rmgr() to handle exactly this scenario. We just need to move it up in bnxt_need_reserve_rings() to be called unconditionally when using older firmware. Without the fix, if the TX rings are changing, we'll skip the bnxt_check_rss_tbl_no_rmgr() call and __bnxt_reserve_rings() may also skip the bnxt_set_dflt_rss_indir_tbl() call for the reason explained		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the last paragraph. Without setting the default RSS indirection table to default, it causes the regression: BUG: KASAN: slab-out-of-bounds in __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 Read of size 2 at addr ffff8881c5809618 by task ethtool/31525 Call Trace: __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 bnxt_hwrm_vnic_rss_cfg_p5+0xf7/0x460 __bnxt_setup_vnic_p5+0x12e/0x270 __bnxt_open_nic+0x2262/0x2f30 bnxt_open_nic+0x5d/0xf0 ethnl_set_channels+0x5d4/0xb30		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ethnl_default_set_doit+0x2f1/0x620 **CVE ID: CVE-2024-44933**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_soc	https://git.kernel.org/stable/c/05e4a0fa248240efd99a539853e844f0f0a9e6a5, https://git.kernel.org/stable/c/1407be30fc17eff918a98e0a990c0e988f11dc84, https://git.kernel.org/stable/c/52319d9d2f522ed939af31af70f8c3a0f0f67e6c	O-LIN-LINU-030924/1132

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint().		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated--- **CVE ID: CVE-2024-44935**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: platform/x86: intel-vbtn: Protect ACPI notify handler against recursion Since commit e2ffcda16290 ("ACPI: OSL: Allow Notify () handlers to run on all CPUs") ACPI notify handlers like the intel-vbtn notify_handler() may run on multiple CPU cores racing with themselves. This race gets hit on Dell Venue 7140 tablets when undocking from the keyboard, causing the handler	https://git.kernel.org/stable/c/5c9618a3b6ea94cf7bdff7702aca8bf2d777d97b , https://git.kernel.org/stable/c/e075c3b13a0a142dcd3151b25d29a24f31b7b640	O-LIN-LINU-030924/1133

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to try and register priv->switches_dev twice, as can be seen from the dev_info() message getting logged twice: [83.861800] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after receiving a switch event [83.861858] input: Intel Virtual Switches as /devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17 [83.861865] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after receiving a switch event After which things go seriously wrong: [83.861872] sysfs: cannot create duplicate filename '/devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17'		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			... [83.861967] kobject: kobject_add_internal failed for input17 with -EEXIST, don't try to register things with the same name in the same directory. [83.877338] BUG: kernel NULL pointer dereference, address: 0000000000000018 ... Protect intel-vbtn notify_handler() from racing with itself with a mutex to fix this. **CVE ID: CVE-2024-44937**		
Affected Version(s): From (including) 2.6.12 Up to (excluding) 4.19.320					
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree **CVE ID: CVE-2024-43858**	https://git.kernel.org/stable/c/538a27c8048f081a5ddd286f886eb986fbbc7f80, https://git.kernel.org/stable/c/55b732c8b09b41148eaab2fa8e31b0af47671e00, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1134

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				63f7fdf733add82f126ea00e2e48f6eba15ac4b9	
Affected Version(s): From (including) 2.6.16 Up to (excluding) 4.9.304					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is: A --> B --> C --> D A <-- B <-- C <-- D delete list_head *B | delete list_head *C	https://git.kernel.org/stable/c/3aadfd46858b1f64d4d6a0654b863e21aabff975, https://git.kernel.org/stable/c/40805099af11f68c5ca7dbcfacf455da8f99f622, https://git.kernel.org/stable/c/84ec758fb2daa236026506868c8796b0500c047d	O-LIN-LINU-030924/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			-------------------------------|---------------------------------- configfs_unregister_subsystem | configfs_unregister_subsystem unlink_group | unlink_group unlink_obj | unlink_obj list_del_init | list_del_init __list_del_entry | __list_del_entry __list_del | __list_del // next == C | next->prev = prev | | next->prev = prev prev->next = next | | // prev == B | prev->next = next Fix this by adding mutex when calling link_group() or unlink_group(), but parent configfs_subsystem is NULL when config_item is root.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			So I create a mutex configfs_subsystem_mutex. **CVE ID: CVE-2022-48931**		
Affected Version(s): From (including) 2.6.21 Up to (excluding) 4.19.320					
Allocation of Resources Without Limits or Throttling	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse, then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list.	https://git.kernel.org/stable/c/1fe97f68fce1ba24bf823bfb0eb0956003473130, https://git.kernel.org/stable/c/22094f5f52e7bc16c5bf9613365049383650b02e, https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7	O-LIN-LINU-030924/1136

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03 **CVE ID: CVE-2024-43856**		
Affected Version(s): From (including) 2.6.27 Up to (excluding) 5.15.165					
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: initialize integrity buffer to zero before writing it to media	https://git.kernel.org/stable/c/23a19655fb56f241e592041156dfb1c6d04da644, https://git.kernel.org/stable/c/899ee2c3829c5ac14bfc7d3c4a5846c0b709b78f,	O-LIN-LINU-030924/1137

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Metadata added by bio_integrity_prep is using plain kmalloc, which leads to random kernel memory being written media. For PI metadata this is limited to the app tag that isn't used by kernel generated metadata, but for non-PI metadata the entire buffer leaks kernel memory. Fix this by adding the __GFP_ZERO flag to allocations for writes. **CVE ID: CVE-2024-43854**	https://git.kernel.org/stable/c/cf6b45ea7a8df0f61bded1dc4a8561ac6ad143d2	
Affected Version(s): From (including) 3.15 Up to (excluding) 4.9.304					
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous	https://git.kernel.org/stable/c/0f88722313645a903f4d420ba61ddc690ec2481d, https://git.kernel.org/stable/c/1aa12ecfdcbafebc218910ec47acf6262e600cf5, https://git.kernel.org/stable/c/53d43a9c8dd224e66559fe86a	O-LIN-LINU-030924/1138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function. **CVE ID: CVE-2022-48928**	f1e473802c7130e	
Affected Version(s): From (including) 3.3 Up to (excluding) 4.19.320					
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes In psb_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	https://git.kernel.org/stable/c/13b5f3ee94bdbdc4b5f40582aab62977905aedee, https://git.kernel.org/stable/c/2df7aac81070987b0f052985856aa325a38debf6, https://git.kernel.org/stable/c/46d2ef272957879cbe30a884574320e7f7d78692	O-LIN-LINU-030924/1139

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42309		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42310**	https://git.kernel.org/stable/c/08f45102c81ad8bc9f85f7a25e9f64e128edb87d, https://git.kernel.org/stable/c/2d209b2f862f6b8bff549ede541590a8d119da23, https://git.kernel.org/stable/c/977ee4fe895e1729cd36cc26916bbb10084713d6	O-LIN-LINU-030924/1140
Affected Version(s): From (including) 3.4 Up to (excluding) 4.19.320					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close()	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa	O-LIN-LINU-030924/1141

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>]	1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding handling is missing. Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv. **CVE ID: CVE-2024-42271**		
Affected Version(s): From (including) 3.8 Up to (excluding) 4.9.304					
Improper Locking	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync() **CVE ID: CVE-2022-48930**	https://git.kernel.org/stable/c/081bdc9fe05bb23248f5effb6f811da3da4b8252, https://git.kernel.org/stable/c/4752fafb461821f8c8581090c923ababba68c5bd, https://git.kernel.org/stable/c/8cc342508f9e7fdccd2e9758ae9d52aff72dab7f	O-LIN-LINU-030924/1142
Affected Version(s): From (including) 4.1 Up to (excluding) 4.19.320					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address. **CVE ID: CVE-2024-42284**	https://git.kernel.org/stable/c/253405541be2f15ffebdeac2f4cf4b7e9144d12f, https://git.kernel.org/stable/c/2abe350db1aa599eeebc6892237d0bce0f1de62a, https://git.kernel.org/stable/c/5eea127675450583680c8170358bcba43227bd69	O-LIN-LINU-030924/1143
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.269					
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption	https://git.kernel.org/stable/c/33222d1571d7ce8c1c75f6b488f38968fa93d2d9, https://git.kernel.org/stable/c/4ce247af3f30078d5b97554f1ae6200a0222c15a, https://git.kernel.org/stable/c/669c2b178956	O-LIN-LINU-030924/1144

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption. next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979]	718407af5631ccbc61c24413f038	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4 [361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979] dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1: irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c **CVE ID: CVE-2022-48926**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function. **CVE ID: CVE-2022-48928**	https://git.kernel.org/stable/c/0f88722313645a903f4d420ba61ddc690ec2481d, https://git.kernel.org/stable/c/1aa12ecfdcbafebc218910ec47acf6262e600cf5, https://git.kernel.org/stable/c/53d43a9c8dd224e66559fe86af1e473802c7130e	O-LIN-LINU-030924/1145
Improper Locking	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock	https://git.kernel.org/stable/c/081bdc9fe05bb23248f5effb6f811da3da4b8252, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1146

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync() **CVE ID: CVE-2022-48930**	4752fafb461821f8c8581090c923ababba68c5bd, https://git.kernel.org/stable/c/8cc342508f9e7fdccd2e9758ae9d52aff72dab7f	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic.	https://git.kernel.org/stable/c/3aadfd46858b1f64d4d6a0654b863e21aabff975, https://git.kernel.org/stable/c/40805099af11f68c5ca7dbcfacf455da8f99f622, https://git.kernel.org/stable/c/84ec758fb2daa236026506868c8796b0500c047d	O-LIN-LINU-030924/1147

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			One of cases is: A --> B --> C --> D A <-- B <-- C <-- D delete list_head *B | delete list_head *C --------------------------------|----------------------------------- configfs_unregister_subsystem | configfs_unregister_subsystem unlink_group | unlink_group unlink_obj | unlink_obj list_del_init | list_del_init __list_del_entry | __list_del_entry __list_del | __list_del // next == C | next->prev = prev | | next->prev = prev prev->next = next | | // prev == B | prev->next = next		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix this by adding mutex when calling link_group() or unlink_group(), but parent configfs_subsystem is NULL when config_item is root. So I create a mutex configfs_subsystem _mutex. **CVE ID: CVE-2022-48931**		
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.270					
Double Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed	https://git.kernel.org/stable/c/147a0e71ccf96df9fc8c2ac500829d8e423ef02c, https://git.kernel.org/stable/c/2fe0e281f7ad0a62259649764228227dd6b2561d, https://git.kernel.org/stable/c/3d6cc9898efdfb062efb74dc18cfc700e082f5d5	O-LIN-LINU-030924/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4 [Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0 [Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0 ... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	__x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae **CVE ID: CVE-2022-48919**		
Affected Version(s): From (including) 4.13 Up to (excluding) 4.19.320					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decoding can incur a read after free for inst. Fix it by cancelling the work in vdec_close. **CVE ID: CVE-2024-42313**	https://git.kernel.org/stable/c/4c9d235630d35db762b85a4149bbb0be9d504c36, https://git.kernel.org/stable/c/66fa52edd32cdbb675f0803b3c4da10ea19b6635, https://git.kernel.org/stable/c/6a96041659e834dc0b172dda4b2df512d63920c2	O-LIN-LINU-030924/1149
Affected Version(s): From (including) 4.14 Up to (excluding) 4.14.270					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/05f7927b25d2635e87267ff6c79db79fb46cf31	O-LIN-LINU-030924/1150

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netfilter: fix use-after-free in __nf_register_net_hook() We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430	3, https://git.kernel.org/stable/c/49c24579cec41e32f13d57b337fd28fb208d4a5b, https://git.kernel.org/stable/c/56763f12b0f02706576a088e85ef856deacc98a0	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #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+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 nf_hook_entries_get_hook_ops		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218 synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0 net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101 ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084 __sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockop		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			t net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xba/0x150 net/socket.c:2188 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: 0033:0x7f65a1ace7d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 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 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9 RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12: 00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000 </TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x35a/0x4a0 mm/slub. ---truncated--- **CVE ID: CVE-2022-48912**		
Affected Version(s): From (including) 4.14 Up to (excluding) 4.14.274					
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: fix memory leak in int3400_notify()	https://git.kernel.org/stable/c/2e798814e01827871938ff172d2b2ccf1e74b355, https://git.kernel.org/stable/c/33c73a4d7e7b19313a6b41715	O-LIN-LINU-030924/1151

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies 4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65 NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b a5 rmal.kkkkkkkkkk. backtrace: [<ffffffff9c502c3e>] __kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0 [<ffffffff9c7b7d6e>]	2f5365016926418, https://git.kernel.org/stable/c/3abea10e6a8f0e7804ed4c124bea2d15aca977c8	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>] acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0 [<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0 [<ffffffff9c2cb4dd>] kthread+0xfd/0x130 [<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly. **CVE ID: CVE-2022-48924**		
Affected Version(s): From (including) 4.14 Up to (excluding) 4.19.320					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node value is NULL In imx_rproc_addr_init() "nph = of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE. [Fixed title to fit within the	https://git.kernel.org/stable/c/2fa26ca8b786888673689ccc9da60941509399 82, https://git.kernel.org/stable/c/4e13b7c23988c0a13fdca92e94296a3bc2ff9f21 , https://git.kernel.org/stable/c/6884fd0283e0831be153fb8d82d9eda8a55acaaa	O-LIN-LINU-030924/1152

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prescribed 70-75 charcters] **CVE ID: CVE-2024-43860**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.232					
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption.	https://git.kernel.org/stable/c/33222d1571d7ce8c1c75f6b488f38968fa93d2d9, https://git.kernel.org/stable/c/4ce247af3f30078d5b97554f1ae6200a0222c15a, https://git.kernel.org/stable/c/669c2b178956718407af5631ccbc61c24413f038	O-LIN-LINU-030924/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4 [361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1: irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c **CVE ID: CVE-2022-48926**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous	https://git.kernel.org/stable/c/0f88722313645a903f4d420ba61ddc690ec2481d, https://git.kernel.org/stable/c/1aa12ecfdcbafebc218910ec47acf6262e600cf5, https://git.kernel.org/stable/c/53d43a9c8dd224e66559fe86a	O-LIN-LINU-030924/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function. **CVE ID: CVE-2022-48928**	f1e473802c7130e	
Improper Locking	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync() **CVE ID: CVE-2022-48930**	https://git.kernel.org/stable/c/081bdc9fe05bb23248f5effb6f811da3da4b8252, https://git.kernel.org/stable/c/4752fafb461821f8c8581090c923ababba68c5bd, https://git.kernel.org/stable/c/8cc342508f9e7fdccd2e9758ae9d52aff72dab7f	O-LIN-LINU-030924/1155
Concurrent Execution using Shared Resource with Improper Synchronization	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in	https://git.kernel.org/stable/c/3aadfd46858b1f64d4d6a0654b863e21aabff975, https://git.kernel.org/stable/c/40805099af11f	O-LIN-LINU-030924/1156

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is: A --> B --> C --> D A <-- B <-- C <-- D delete list_head *B | delete list_head *C --------------------------------|---------------------------------- configfs_unregister_subsystem | configfs_unregister_subsystem unlink_group | unlink_group unlink_obj | unlink_obj	68c5ca7dbcfacf455da8f99f622, https://git.kernel.org/stable/c/84ec758fb2daa236026506868c8796b0500c047d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			list_del_init
			| list_del_init
			__list_del_entry
			|
			__list_del_entry
			__list_del |
			__list_del
			// next == C
			|
			next->prev = prev |
			|
			next->prev = prev
			prev->next = next |
			|
			// prev == B
			|
			prev->next = next
			
			Fix this by adding mutex when calling link_group() or unlink_group(),
			but parent configfs_subsystem is NULL when config_item is root.
			So I create a mutex configfs_subsystem_mutex.
			CVE ID: CVE-2022-48931		

Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.233					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/05f7927b25d2635e87267ff6c79db79fb46cf31	O-LIN-LINU-030924/1157

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	netfilter: fix use-after-free in __nf_register_net_hook() We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430	3, https://git.kernel.org/stable/c/49c24579cec41e32f13d57b337fd28fb208d4a5b, https://git.kernel.org/stable/c/56763f12b0f02706576a088e85ef856deacc98a0	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #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+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 nf_hook_entries_get_hook_ops		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218 synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0 net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101 ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084 __sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockop		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			t net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xba/0x150 net/socket.c:2188 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: 0033:0x7f65a1ace7d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 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 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9 RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12: 00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000 </TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x35a/0x4a0 mm/slub. ---truncated--- **CVE ID: CVE-2022-48912**		
Double Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root()	https://git.kernel.org/stable/c/147a0e71ccf96df9fc8c2ac500829d8e423ef02c, https://git.kernel.org/stable/c/2fe0e281f7ad0a62259649764228227dd6b2561d,	O-LIN-LINU-030924/1158

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4	https://git.kernel.org/stable/c/3d6cc9898efdfb062efb74dc18cfc700e082f5d5	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae **CVE ID: CVE-2022-48919**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.237					
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: fix memory leak in int3400_notify() It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies 4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65	https://git.kernel.org/stable/c/2e798814e01827871938ff172d2b2ccf1e74b355, https://git.kernel.org/stable/c/33c73a4d7e7b19313a6b417152f5365016926418, https://git.kernel.org/stable/c/3abea10e6a8f0e7804ed4c124bea2d15aca977c8	O-LIN-LINU-030924/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b a5 rmal.kkkkkkkkkk. backtrace: [<ffffffff9c502c3e>] __kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0 [<ffffffff9c7b7d6e>] kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>] acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0 [<ffffffff9c2cb4dd>] kthread+0xfd/0x130 [<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly. **CVE ID: CVE-2022-48924**		
Affected Version(s): From (including) 4.19.142 Up to (excluding) 4.19.270					
NULL Pointer Dereference	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: efi: fix NULL-deref in init error path In cases where runtime services are not supported or have been disabled, the runtime services workqueue will never have been allocated.	https://git.kernel.org/stable/c/4ca71bc0e1995d15486cd7b60845602a28399cb5, https://git.kernel.org/stable/c/585a0b2b3ae7903c6abee3087d09c69e955a7794, https://git.kernel.org/stable/c/5fcf75a8a4c3e7ee9122d143684083c9faf20452	O-LIN-LINU-030924/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Do not try to destroy the workqueue unconditionally in the unlikely event that EFI initialisation fails to avoid dereferencing a NULL pointer. **CVE ID: CVE-2022-48879**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.182					
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent	https://git.kernel.org/stable/c/33222d1571d7ce8c1c75f6b488f38968fa93d2d9, https://git.kernel.org/stable/c/4ce247af3f30078d5b97554f1ae6200a0222c15a , https://git.kernel.org/stable/c/669c2b178956718407af5631ccbc61c24413f038	O-LIN-LINU-030924/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption. next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979] dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1: irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c **CVE ID: CVE-2022-48926**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix	https://git.kernel.org/stable/c/0f88722313645a903f4d420ba61ddc690ec2481d, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1162

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a resource leak in an error handling path If iio_device_register() fails, a previous ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function. **CVE ID: CVE-2022-48928**	1aa12ecfdcbafebc218910ec47acf6262e600cf5, https://git.kernel.org/stable/c/53d43a9c8dd224e66559fe86af1e473802c7130e	
Improper Locking	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync() **CVE ID: CVE-2022-48930**	https://git.kernel.org/stable/c/081bdc9fe05bb23248f5effb6f811da3da4b8252, https://git.kernel.org/stable/c/4752fafb461821f8c8581090c923ababba68c5bd, https://git.kernel.org/stable/c/8cc342508f9e7fdccd2e9758ae9d52aff72dab7f	O-LIN-LINU-030924/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is: A --> B --> C --> D A <-- B <-- C <-- D delete list_head *B | delete list_head *C --------------------------------|----------------------------------- configfs_unregister_subsystem |	https://git.kernel.org/stable/c/3aadfd46858b1f64d4d6a0654b863e21aabff975, https://git.kernel.org/stable/c/40805099af11f68c5ca7dbcfacf455da8f99f622, https://git.kernel.org/stable/c/84ec758fb2daa236026506868c8796b0500c047d	O-LIN-LINU-030924/1164

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configfs_unregister_subsystem unlink_group | unlink_group unlink_obj | unlink_obj list_del_init | list_del_init __list_del_entry | __list_del_entry __list_del | __list_del // next == C | next->prev = prev | | next->prev = prev prev->next = next | | // prev == B | prev->next = next Fix this by adding mutex when calling link_group() or unlink_group(), but parent configfs_subsystem is NULL when config_item is root. So I create a mutex configfs_subsystem_mutex.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48931		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.183					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: fix use-after-free in __nf_register_net_hook() We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438	https://git.kernel.org/stable/c/05f7927b25d2635e87267ff6c79db79fb46cf313, https://git.kernel.org/stable/c/49c24579cec41e32f13d57b337fd28fb208d4a5b, https://git.kernel.org/stable/c/56763f12b0f02706576a088e85ef856deacc98a0	O-LIN-LINU-030924/1165

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430 CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #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+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/kasan/report.c:459 nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218 synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline] find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101 ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xba/0x150 net/socket.c:2188 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: 0033:0x7f65a1ace7d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 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		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9 RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12: 00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			</TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETR		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Y|__GFP_COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993 prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x35a/0x4a0 mm/slub. ---truncated--- **CVE ID: CVE-2022-48912**		
Double Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/147a0e71ccf96df9fc8c2ac500829d8e423ef02c,	O-LIN-LINU-030924/1166

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0	https://git.kernel.org/stable/c/2fe0e281f7ad0a62259649764228227dd6b2561d, https://git.kernel.org/stable/c/3d6cc9898efdfb062efb74dc18cfc700e082f5d5	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4 [Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0 [Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0 ... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae **CVE ID: CVE-2022-48919**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.188					
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: fix memory leak in int3400_notify() It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies	https://git.kernel.org/stable/c/2e798814e01827871938ff172d2b2ccf1e74b355, https://git.kernel.org/stable/c/33c73a4d7e7b19313a6b417152f53650169264 18, https://git.kernel.org/stable/c/3abea10e6a8f0e7804ed4c124bea2d15aca977c8	O-LIN-LINU-030924/1167

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65 NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b a5 rmal.kkkkkkkkkk. backtrace: [<ffffffff9c502c3e>] __kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0 [<ffffffff9c7b7d6e>] kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0 [<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0 [<ffffffff9c2cb4dd>] kthread+0xfd/0x130 [<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly. **CVE ID: CVE-2022-48924**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.262					
Use After Free	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unregister flowtable hooks on netns exit Unregister flowtable hooks before they are releases via	https://git.kernel.org/stable/c/6069da443bf65f513bb507bb21e2f87cfb1ad0b6 , https://git.kernel.org/stable/c/88c795491bf45a8c08a0f94c9ca4f13722e51013 , https://git.kernel.org/stable/c/8ffb8ac3448845f65634889b05	O-LIN-LINU-030924/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nf_tables_flowtable_destroy() otherwise hook core reports UAF. BUG: KASAN: use-after-free in nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 Read of size 4 at addr ffff8880736f7438 by task syz-executor579/3666 CPU: 0 PID: 3666 Comm: syz-executor579 Not tainted 5.16.0-rc5-syzkaller #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 lib/dump_stack.c:88 [inline]	1bd65e4dee484b	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lib/dump_stack.c:106 dump_stack_lvl+0x1dc/0x2d8 lib/dump_stack.c:106 lib/dump_stack.c:106 print_address_description+0x65/0x380 mm/kasan/report.c:247 mm/kasan/report.c:247 __kasan_report mm/kasan/report.c:433 [inline] __kasan_report mm/kasan/report.c:433 [inline] mm/kasan/report.c:450 kasan_report+0x19a/0x1f0 mm/kasan/report.c:450 mm/kasan/report.c:450 nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 __nf_register_net_hook+0x27e/0x8d0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/core.c:429 net/netfilter/core.c:429 nf_register_net_hook+0xaa/0x180 net/netfilter/core.c:571 net/netfilter/core.c:571 nft_register_flowtable_net_hooks+0x3c5/0x730 net/netfilter/nf_tables_api.c:7232 net/netfilter/nf_tables_api.c:7232 nf_tables_newflowtable+0x2022/0x2cf0 net/netfilter/nf_tables_api.c:7430 net/netfilter/nf_tables_api.c:7430 nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] net/netfilter/nfnetlink.c:652		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv+0x10e6/0x2550 net/netfilter/nfnetlink.c:652 net/netfilter/nfnetlink.c:652 __nft_release_hook() calls nft_unregister_flowtable_net_hooks() which only unregisters the hooks, then after RCU grace period, it is guaranteed that no packets add new entries to the flowtable (no flow offload rules and flowtable hooks are reachable from packet path), so it is safe to call nf_flow_table_free() which cleans up the remaining entries from the flowtable (both software and hardware) and it unbinds		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the flow_block. **CVE ID: CVE-2022-48935**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.282					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	O-LIN-LINU-030924/1169

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for sock_owned_by_user() and corresponding handling is missing. Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv. **CVE ID: CVE-2024-42271**		
Improper Check for Unusual or Exceptional Conditions	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return	https://git.kernel.org/stable/c/253405541be2f15ffebdeac2f4cf4b7e9144d12f, https://git.kernel.org/stable/c/2abe350db1aa599eeebc6892237d0bce0f1de62a, https://git.kernel.org/stable/c/5eea127675450	O-LIN-LINU-030924/1170

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address. **CVE ID: CVE-2024-42284**	583680c8170358bcba43227bd69	

Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:
			RDMA/iwcm: Fix a use-after-free related to destroying CM IDs
			iw_conn_req_handler() associates a new struct rdma_id_private (conn_id) with
			an existing struct iw_cm_id (cm_id) as follows:
			conn_id->cm_id.iw = cm_id;
			cm_id->context = conn_id;
			cm_id->cm_handler = cma_iw_handler;
				https://git.kernel.org/stable/c/557d035fe88d78dd51664f4dc0e1896c04c97cf6, https://git.kernel.org/stable/c/7f25f296fc9bd0435be14e89bf657cd615a23574, https://git.kernel.org/stable/c/94ee7ff99b87435ec63211f632918dc7f44dac79	O-LIN-LINU-030924/1171

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdma_destroy_id() frees both the cm_id and the struct rdma_id_private. Make sure that cm_work_handler() does not trigger a use-after-free by only freeing of the struct rdma_id_private after all pending work has finished. **CVE ID: CVE-2024-42285**		
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered	https://git.kernel.org/stable/c/166a0bddcc27de41fe13f861c8348e8e53e988c8, https://git.kernel.org/stable/c/47b3dce100778001cd76f7e9188944b5cb27a76d, https://git.kernel.org/stable/c/7789a1d6792af410aa9b39a1eb237ed24fa2170a	O-LIN-LINU-030924/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QThread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dump_backtrace+0x0/0x1c0 [66.575469s][pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s][pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s][pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s][pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s][pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport] **CVE ID: CVE-2024-42301**		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close	https://git.kernel.org/stable/c/4c9d235630d35db762b85a4149bbb0be9d504c36, https://git.kernel.org/stable/c/66fa52edd32cdbb675f0803b3c4da10ea19b6635,	O-LIN-LINU-030924/1173

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decoding can incur a read after free for inst. Fix it by cancelling the work in vdec_close. **CVE ID: CVE-2024-42313**	https://git.kernel.org/stable/c/6a96041659e834dc0b172dda4b2df512d63920c2	
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree **CVE ID: CVE-2024-43858**	https://git.kernel.org/stable/c/538a27c8048f081a5ddd286f886eb986fbbc7f80, https://git.kernel.org/stable/c/55b732c8b09b41148eaab2fa8e31b0af47671e00, https://git.kernel.org/stable/c/63f7fdf733add8	O-LIN-LINU-030924/1174

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2f126ea00e2e48f6eba15ac4b9	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed when receiving ICMP packets with secmark set while an ICMP raw socket is being created. SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socket before that, causing the null pointer dereference. Drop the packet if label context is not set. BUG: kernel NULL pointer dereference, address:	https://git.kernel.org/stable/c/0abe35bc48d4ec80424b1f4b3560c0e082cbd5c1, https://git.kernel.org/stable/c/290a6b88e8c19b6636ed1acc733d1458206f7697, https://git.kernel.org/stable/c/347dcb84a4874b5fb375092c08d8cc4069b94f81	O-LIN-LINU-030924/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			000000000000004c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1 3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 RIP: 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 89 f0 <8b> 77 4c 39 c6 7e 1f 48 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 000000000000000e RDX: ffffa92940003be8 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400 R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 R12: ffff8b574c642400 R13: 0000000000000001 R14: 0000000000000001 R15: 0000000000000000 FS: 00007fb092ea7640(0000) GS:ffff8b577bc000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	00(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40 apparmor_secmark_check+0xec/0x330 security_sock_rcv_skb+0x35/0x50		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0 ip_local_deliver_finish+0x76/0xa0 __netif_receive_skb_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 net_rx_action+0x2a4/0x380 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0 common_interrupt+0x86/0xa0 </IRQ> <TASK> asm_common_interrupt+0x26/0x40 RIP: 0010:apparmor_socket_post_create+0xb/0x200 Code: 08 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00 00 48 8b 1d 80 56 3f 02 48 RSP: 0018:ffffa92940ce		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000002 RDI: ffff8b574eaab740 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 0000000000000002 R14: ffff8b574eaab740 R15: ffffffffbd8e4748 ? __pfx_apparmor_socket_post_create+0x10/0x10 security_socket_po		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			st_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys_socket+0x89/0x100 __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc **CVE ID: CVE-2023-52889**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes	https://git.kernel.org/stable/c/13b5f3ee94bdbdc4b5f40582aab62977905aedee, https://git.kernel.org/stable/c/2df7aac81070987b0f052985856aa325a38debf6,	O-LIN-LINU-030924/1176

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In psb_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42309**	https://git.kernel.org/stable/c/46d2ef272957879cbe30a884574320e7f7d78692	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on	https://git.kernel.org/stable/c/08f45102c81ad8bc9f85f7a25e9f64e128edb87d, https://git.kernel.org/stable/c/2d209b2f862f6b8bff549ede541590a8d119da23, https://git.kernel.org/stable/c/977ee4fe895e1729cd36cc26916bbb10084713d6	O-LIN-LINU-030924/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42310**		
Allocation of Resources Without Limits or Throttling	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse, then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list. If this happens, there will be two	https://git.kernel.org/stable/c/1fe97f68fce1ba24bf823bfb0eb0956003473130, https://git.kernel.org/stable/c/22094f5f52e7bc16c5bf9613365049383650b02e, https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7	O-LIN-LINU-030924/1178

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03 **CVE ID: CVE-2024-43856**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node value is NULL In imx_rproc_addr_init() "nph =	https://git.kernel.org/stable/c/2fa26ca8b786888673689ccc9da6094150939982, https://git.kernel.org/stable/c/4e13b7c23988c0a13fdca92e94296a3bc2ff9f21, https://git.kernel.org/stable/c/6884fd0283e0831be153fb8d82	O-LIN-LINU-030924/1179

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE. [Fixed title to fit within the prescribed 70-75 charcters] **CVE ID: CVE-2024-43860**	d9eda8a55acaaa	
Affected Version(s): From (including) 4.3 Up to (including) 6.10.6					
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Add error handling to pair_device()	https://git.kernel.org/stable/c/538fd3921afac97158d4177139a0ad39f056dbb2	O-LIN-LINU-030924/1180

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hci_conn_params_add() never checks for a NULL value and could lead to a NULL pointer dereference causing a crash. Fixed by adding error handling in the function. **CVE ID: CVE-2024-43884**		
Affected Version(s): From (including) 4.6 Up to (excluding) 4.9.304					
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent	https://git.kernel.org/stable/c/33222d1571d7ce8c1c75f6b488f38968fa93d2d9, https://git.kernel.org/stable/c/4ce247af3f30078d5b97554f1ae6200a0222c15a , https://git.kernel.org/stable/c/669c2b178956718407af5631ccbc61c24413f038	O-LIN-LINU-030924/1181

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption. next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979] dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1: irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c **CVE ID: CVE-2022-48926**		
Affected Version(s): From (including) 4.6 Up to (excluding) 6.1.103					
Use After Free	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1be59c97c83ccd67a519d8a49486b3a8a73ca28a,	O-LIN-LINU-030924/1182

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cgroup/cpuset: Prevent UAF in proc_cpuset_show() An UAF can happen when /proc/cpuset is read as reported in [1]. This can be reproduced by the following methods: 1.add an mdelay(1000) before acquiring the cgroup_lock In the cgroup_path_ns function. 2.$cat /proc/<pid>/cpuset repeatly. 3.$mount -t cgroup -o cpuset cpuset /sys/fs/cgroup/cpuset/ $umount /sys/fs/cgroup/cpuset/ repeatly. The race that cause this bug can be shown as below: (umount) | (cat /proc/<pid>/cpuset)	https://git.kernel.org/stable/c/29a8d4e02fd4840028c38ceb1536cc8f82a257d4, https://git.kernel.org/stable/c/29ac1d238b3bf126af36037df80d7ecc4822341e	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			css_release | proc_cpuset_show
			css_release_work_fn | css = task_get_css(tsk, cpuset_cgrp_id);
			css_free_rwork_fn | cgroup_path_ns(css->cgroup, ...);
			cgroup_destroy_root | mutex_lock(&cgroup_mutex);
			rebind_subsystems |
			cgroup_free_root |
			| // cgrp was freed, UAF
			| cgroup_path_ns_locked(cgrp,..);
			When the cpuset is initialized, the root node top_cpuset.css.cgrp
			will point to &cgrp_dfl_root.cgrp. In cgroup v1, the mount operation will
			allocate cgroup_root, and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			top_cpuset.css.cgrp will point to the allocated &cgroup_root.cgrp. When the umount operation is executed, top_cpuset.css.cgrp will be rebound to &cgrp_dfl_root.cgrp. The problem is that when rebinding to cgrp_dfl_root, there are cases where the cgroup_root allocated by setting up the root for cgroup v1 is cached. This could lead to a Use-After-Free (UAF) if it is subsequently freed. The descendant cgroups of cgroup v1 can only be freed after the css is released. However, the css of the root will never be released, yet the cgroup_root should be freed when it is unmounted. This means that obtaining a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reference to the css of the root does not guarantee that css.cgrp->root will not be freed. Fix this problem by using rcu_read_lock in proc_cpuset_show(). As cgroup_root is kfree_rcu after commit d23b5c577715 ("cgroup: Make operations on the cgroup root_list RCU safe"), css->cgroup won't be freed during the critical section. To call cgroup_path_ns_locked, css_set_lock is needed, so it is safe to replace task_get_css with task_css. [1] https://syzkaller.appspot.com/bug?extid=9b1ff7be974a403aa4cd **CVE ID: CVE-2024-43853**		
Affected Version(s): From (including) 4.8 Up to (excluding) 4.19.320					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:
			RDMA/iwcm: Fix a use-after-free related to destroying CM IDs
			iw_conn_req_handler() associates a new struct rdma_id_private (conn_id) with
			an existing struct iw_cm_id (cm_id) as follows:
			conn_id->cm_id.iw = cm_id;
			cm_id->context = conn_id;
			cm_id->cm_handler = cma_iw_handler;
			rdma_destroy_id() frees both the cm_id and the struct rdma_id_private. Make
			sure that cm_work_handler() does not trigger a use-after-free by only
			freeing of the struct rdma_id_private
				https://git.kernel.org/stable/c/557d035fe88d78dd51664f4dc0e1896c04c97cf6, https://git.kernel.org/stable/c/7f25f296fc9bd0435be14e89bf657cd615a23574, https://git.kernel.org/stable/c/94ee7ff99b87435ec63211f632918dc7f44dac79	O-LIN-LINU-030924/1183

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after all pending work has finished. **CVE ID: CVE-2024-42285**		
Affected Version(s): From (including) 5.0 Up to (excluding) 5.4.282					
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_soc	https://git.kernel.org/stable/c/05e4a0fa248240efd99a539853e844f0f0a9e6a5 , https://git.kernel.org/stable/c/1407be30fc17eff918a98e0a990c0e988f11dc84, https://git.kernel.org/stable/c/52319d9d2f522ed939af31af70f8c3a0f0f67e6c	O-LIN-LINU-030924/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint().		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	RIP: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated--- **CVE ID: CVE-2024-44935**		
Affected Version(s): From (including) 5.1 Up to (excluding) 5.4.182					
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: flower: Fix a potential leak in nfp_tunnel_add_shared_mac() ida_simple_get() returns an id between min (0) and max (NFP_MAX_MAC_INDEX) inclusive. So NFP_MAX_MAC_INDEX (0xff) is a valid id. In order for the error handling path to work correctly, the 'invalid' value for 'ida_idx' should not be in the	https://git.kernel.org/stable/c/3a14d0888eb4b0045884126acc69abfb7b87814d, https://git.kernel.org/stable/c/4086d2433576baf85f0e538511df97c8101e0a10, https://git.kernel.org/stable/c/5ad5886f85b6bd893e3ed19013765fb0c243c069	O-LIN-LINU-030924/1185

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0..NFP_MAX_MAC_INDEX range, inclusive. So set it to -1. **CVE ID: CVE-2022-48934**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.10.103					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/cma: Do not change route.addr.src_addr outside state checks If the state is not idle then resolve_prepare_src() should immediately fail and no change to global state should happen. However, it unconditionally overwrites the src_addr trying to build a temporary any address. For instance if the state is already RDMA_CM_LISTEN	https://git.kernel.org/stable/c/00265efbd3e5705038c9492a434fda8cf960c8a2, https://git.kernel.org/stable/c/22e9f71072fa605cbcf033158db58e0790101928d, https://git.kernel.org/stable/c/5b1cef5798b4fd6e4fd5522e7b8a26248beecaa	O-LIN-LINU-030924/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	then this will corrupt the src_addr and would cause the test in cma_cancel_operation(): if (cma_any_addr(cma_src_addr(id_priv)) && !id_priv->cma_dev) Which would manifest as this trace from syzkaller: BUG: KASAN: use-after-free in __list_add_valid+0x93/0xa0 lib/list_debug.c:26 Read of size 8 at addr ffff8881546491e0 by task syz-executor.1/32204 CPU: 1 PID: 32204 Comm: syz-executor.1 Not tainted 5.12.0-rc8-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIOS Google 01/01/2011 Call Trace: __dump_stack lib/dump_stack.c:79 [inline] dump_stack+0x141/0x1d7 lib/dump_stack.c:120 print_address_description.constprop.0.cold+0x5b/0x2f8 mm/kasan/report.c:232 __kasan_report mm/kasan/report.c:399 [inline] kasan_report.cold+0x7c/0xd8 mm/kasan/report.c:416 __list_add_valid+0x93/0xa0 lib/list_debug.c:26 __list_add include/linux/list.h:67 [inline] list_add_tail include/linux/list.h:100 [inline] cma_listen_on_all drivers/infiniband/core/cma.c:2557 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdma_listen+0x787/0xe00 drivers/infiniband/core/cma.c:3751 ucma_listen+0x16a/0x210 drivers/infiniband/core/ucma.c:1102 ucma_write+0x259/0x350 drivers/infiniband/core/ucma.c:1732 vfs_write+0x28e/0xa30 fs/read_write.c:603 ksys_write+0x1ee/0x250 fs/read_write.c:658 do_syscall_64+0x2d/0x70 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x44/0xae This is indicating that an rdma_id_private was destroyed without doing		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cma_cancel_listens(). Instead of trying to re-use the src_addr memory to indirectly create an any address derived from the dst build one explicitly on the stack and bind to that as any other normal flow would do. rdma_bind_addr() will copy it over the src_addr once it knows the state is valid. This is similar to commit bc0bdc5afaa7 ("RDMA/cma: Do not change route.addr.src_addr.ss_family") **CVE ID: CVE-2022-48925**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.10.224					
Loop with Unreachable Exit Condition ('Infinite Loop')	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ext4: fix infinite loop when	https://git.kernel.org/stable/c/0619f7750f2b178a1309808832ab20d85e0ad121, https://git.kernel.org/stable/c/181e63cd595c6	O-LIN-LINU-030924/1187

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	replaying fast_commit When doing fast_commit replay an infinite loop may occur due to an uninitialized extent_status struct. ext4_ext_determine_insert_hole() does not detect the replay and calls ext4_es_find_extent_range(), which will return immediately without initializing the 'es' variable. Because 'es' contains garbage, an integer overflow may happen causing an infinite loop in this function, easily reproducible using fstest generic/039. This commit fixes this issue by unconditionally initializing the structure in function ext4_es_find_extent_range().	88194e07332f9944b3a63193de2, https://git.kernel.org/stable/c/5ed0496e383cb6de120e56991385dce70bbb87c1	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thanks to Zhang Yi, for figuring out the real problem! **CVE ID: CVE-2024-43828**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.15.165					
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: wait for previous gc cycles when removing port syzbot hit a use-after-free[1] which is caused because the bridge doesn't make sure that all previous garbage has been collected when removing a port. What happens is: CPU 1 CPU 2 start gc cycle remove port acquire gc lock first wait for lock call br_multicasg_gc() directly acquire lock now but free port	https://git.kernel.org/stable/c/0d8b26e10e680c01522d7cc14abe04c3265a928f, https://git.kernel.org/stable/c/1e16828020c674b3be85f52685e8b80f9008f50f, https://git.kernel.org/stable/c/92c4ee25208d0f35dafc3213cdf355fbe449e078	O-LIN-LINU-030924/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the port can be freed while grp timers still running Make sure all previous gc cycles have finished by using flush_work before freeing the port. [1] BUG: KASAN: slab-use-after-free in br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 Read of size 8 at addr ffff888071d6d000 by task syz.5.1232/9699 CPU: 1 PID: 9699 Comm: syz.5.1232 Not tainted 6.10.0-rc5-syzkaller-00021-g24ca36a562d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 call_timer_fn+0x1a3/0x610 kernel/time/timer.c:1792 expire_timers kernel/time/timer.c:1843 [inline] __run_timers+0x74		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			b/0xaf0 kernel/time/timer.c:2417 __run_timer_base kernel/time/timer.c:2428 [inline] __run_timer_base kernel/time/timer.c:2421 [inline] run_timer_base+0x111/0x190 kernel/time/timer.c:2437 **CVE ID: CVE-2024-44934**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.165					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed).	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	O-LIN-LINU-030924/1189

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding handling is missing. Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42271		
Improper Check for Unusual or Exceptional Conditions	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address. **CVE ID: CVE-2024-42284**	https://git.kernel.org/stable/c/253405541be2f15ffebdeac2f4cf4b7e9144d12f, https://git.kernel.org/stable/c/2abe350db1aa599eeebc6892237d0bce0f1de62a, https://git.kernel.org/stable/c/5eea127675450583680c8170358bcba43227bd69	O-LIN-LINU-030924/1190
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix a use-after-free related to destroying CM IDs iw_conn_req_handler() associates a	https://git.kernel.org/stable/c/557d035fe88d78dd51664f4dc0e1896c04c97cf6, https://git.kernel.org/stable/c/7f25f296fc9bd0435be14e89bf657cd615a23574, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1191

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			new struct rdma_id_private (conn_id) with
			an existing struct iw_cm_id (cm_id) as follows:
			conn_id->cm_id.iw = cm_id;
			cm_id->context = conn_id;
			cm_id->cm_handler = cma_iw_handler;
			rdma_destroy_id() frees both the cm_id and the struct rdma_id_private. Make
			sure that cm_work_handler() does not trigger a use-after-free by only
			freeing of the struct rdma_id_private after all pending work has finished.
			CVE ID: CVE-2024-42285
				94ee7ff99b87435ec63211f632918dc7f44dac79	

Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/166a0bddcc27de41fe13f861c8348e8e53e988c8 , https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1192

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID:	47b3dce100778001cd76f7e9188944b5cb27a76d, https://git.kernel.org/stable/c/7789a1d6792af410aa9b39a1eb237ed24fa2170a	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QThread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9] dump_backtrace+0x0/0x1c0 [66.575469s] [pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s] [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QT		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hread,4] do_hardware_base_addr+0xcc/0xd0 [parport] **CVE ID: CVE-2024-42301**		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a DPC event occurs concurrently to hot-removal of the same portion of the hierarchy: The dpc_handler() awaits readiness of the secondary bus below the Downstream Port where the DPC event occurred. To do so, it polls the config space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct pci_dev	https://git.kernel.org/stable/c/11a1f4bc47362700fcbde717292158873fb847ed, https://git.kernel.org/stable/c/2c111413f38ca5cf87557cab89f6d82b0e3433e7, https://git.kernel.org/stable/c/2cc8973bdc4d6c928ebe38b88090a2cdfe81f42f	O-LIN-LINU-030924/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause the kernel to oops. That's because pci_bridge_wait_for_secondary_bus() neglects to hold a reference on the child device. Before v6.3, the function was only called on resume from system sleep or on runtime resume. Holding a reference wasn't necessary back then because the pciehp IRQ thread could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the resume_noirq phase. And runtime resume is always awaited before a PCI device is removed.) However starting with v6.3, pci_bridge_wait_for_secondary_bus() is also called on a DPC event. Commit		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			53b54ad074de ("PCI/DPC: Await readiness of secondary bus after reset"), which introduced that, failed to appreciate that pci_bridge_wait_for_secondary_bus() now needs to hold a reference on the child device because dpc_handler() and pciehp may indeed run concurrently. The commit was backported to v5.10+ stable kernels, so that's the oldest one affected. Add the missing reference acquisition. Abridged stack trace: BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464 Comm: irq/53-pcie-dpc 6.9.0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			RIP: pci_bus_read_config_dword+0x17/0x50
			pci_dev_wait()
			pci_bridge_wait_for_secondary_bus()
			dpc_reset_link()
			pcie_do_recovery()
			dpc_handler()
			CVE ID: CVE-2024-42302		

Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace	https://git.kernel.org/stable/c/4c9d235630d35db762b85a4149bbb0be9d504c36, https://git.kernel.org/stable/c/66fa52edd32cdbb675f0803b3c4da10ea19b6635, https://git.kernel.org/stable/c/6a96041659e834dc0b172dda4b2df512d63920c2	O-LIN-LINU-030924/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during normal decoding can incur a read after free for inst. Fix it by cancelling the work in vdec_close. **CVE ID: CVE-2024-42313**		
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree **CVE ID: CVE-2024-43858**	https://git.kernel.org/stable/c/538a27c8048f081a5ddd286f886eb986fbbc7f80, https://git.kernel.org/stable/c/55b732c8b09b41148eaab2fa8e31b0af47671e00, https://git.kernel.org/stable/c/63f7fdf733add82f126ea00e2e48f6eba15ac4b9	O-LIN-LINU-030924/1195
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed when receiving ICMP	https://git.kernel.org/stable/c/0abe35bc48d4ec80424b1f4b3560c0e082cbd5c1, https://git.kernel.org/stable/c/290a6b88e8c19b6636ed1acc733d1458206f7697, https://git.kernel.org/stable/c/347dcb84a4874	O-LIN-LINU-030924/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	packets with secmark set while an ICMP raw socket is being created. SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socket before that, causing the null pointer dereference. Drop the packet if label context is not set. BUG: kernel NULL pointer dereference, address: 000000000000004c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1	b5fb375092c08d8cc4069b94f81	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 RIP: 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 89 f0 <8b> 77 4c 39 c6 7e 1f 48 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2 RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 000000000000000e RDX: ffffa92940003be8 RSI: 0000000000000000 RDI:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400 R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 R12: ffff8b574c642400 R13: 0000000000000001 R14: 0000000000000001 R15: 0000000000000000 FS: 00007fb092ea7640(0000) GS:ffff8b577bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40 apparmor_secmark_check+0xec/0x330 security_sock_rcv_skb+0x35/0x50 sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_local_deliver_finish+0x76/0xa0 __netif_receive_skb_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 net_rx_action+0x2a4/0x380 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common_interrupt+0x86/0xa0 </IRQ> <TASK> asm_common_interrupt+0x26/0x40 RIP: 0010:apparmor_socket_post_create+0xb/0x200 Code: 08 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00 00 48 8b 1d 80 56 3f 02 48 RSP: 0018:ffffa92940ce7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000002 RDI: ffff8b574eaab740		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 0000000000000002 R14: ffff8b574eaab740 R15: ffffffffbd8e4748 ? __pfx_apparmor_socket_post_create+0x10/0x10 security_socket_post_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys_socket+0x89/0x100 __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc **CVE ID: CVE-2023-52889**		
Use of Uninitialized Resource	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: Initialize all fields in dumped nexthops struct nexthop_grp contains two reserved fields that are not initialized by nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity): # ip nexthop add id 1 dev lo	https://git.kernel.org/stable/c/1377de719652d868f5317ba8398b7e74c5f0430b, https://git.kernel.org/stable/c/5cc4d71dda2dd4f1520f40e634a527022e48ccd8, https://git.kernel.org/stable/c/6d745cd0e9720282cd291d36b9db528aea18add2	O-LIN-LINU-030924/1197

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			# ip nexthop add id 101 group 1 # strace -e recvmsg ip nexthop get id 101 ... recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52 The fields are reserved and therefore not currently used. But as they are, they leak kernel memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure. **CVE ID: CVE-2024-42283**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in	https://git.kernel.org/stable/c/13b5f3ee94bdbdc4b5f40582aab62977905aedee, https://git.kernel.org/stable/c/2df7aac810709	O-LIN-LINU-030924/1198

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			psb_intel_lvds_get_modes In psb_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42309**	87b0f052985856aa325a38debf6, https://git.kernel.org/stable/c/46d2ef272957879cbe30a884574320e7f7d78692	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL	https://git.kernel.org/stable/c/08f45102c81ad8bc9f85f7a25e9f64e128edb87d, https://git.kernel.org/stable/c/2d209b2f862f6b8bff549ede541590a8d119da23, https://git.kernel.org/stable/c/977ee4fe895e1729cd36cc26916bbb10084713d6	O-LIN-LINU-030924/1199

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42310**		
Loop with Unreachable Exit Condition ('Infinite Loop')	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ext4: fix infinite loop when replaying fast_commit When doing fast_commit replay an infinite loop may occur due to an uninitialized extent_status struct. ext4_ext_determine_insert_hole() does not detect the replay and calls ext4_es_find_extent_range(), which will return immediately without initializing the 'es' variable. Because 'es' contains garbage, an integer overflow may happen causing an	https://git.kernel.org/stable/c/0619f7750f2b178a1309808832ab20d85e0ad121, https://git.kernel.org/stable/c/181e63cd595c688194e07332f9944b3a63193de2, https://git.kernel.org/stable/c/5ed0496e383cb6de120e56991385dce70bbb87c1	O-LIN-LINU-030924/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			infinite loop in this function, easily reproducible using fstest generic/039. This commit fixes this issue by unconditionally initializing the structure in function ext4_es_find_extent_range(). Thanks to Zhang Yi, for figuring out the real problem! **CVE ID: CVE-2024-43828**		
Allocation of Resources Without Limits or Throttling	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse, then calls devres_destroy() to remove and free the data structure	https://git.kernel.org/stable/c/1fe97f68fce1ba24bf823bfb0eb0956003473130, https://git.kernel.org/stable/c/22094f5f52e7bc16c5bf9613365049383650b02e, https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7	O-LIN-LINU-030924/1201

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list. If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03 **CVE ID: CVE-2024-43856**		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node value is NULL In imx_rproc_addr_init() "nph = of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE. [Fixed title to fit within the	https://git.kernel.org/stable/c/2fa26ca8b786888673689ccc9da6094150939982, https://git.kernel.org/stable/c/4e13b7c23988c0a13fdca92e94296a3bc2ff9f21, https://git.kernel.org/stable/c/6884fd0283e0831be153fb8d82d9eda8a55acaaa	O-LIN-LINU-030924/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prescribed 70-75 charcters] **CVE ID: CVE-2024-43860**		
Divide By Zero	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time. [10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1 [10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021	https://git.kernel.org/stable/c/6d45e1c948a8b7ed6ceddb14319af69424db730c, https://git.kernel.org/stable/c/8f5ffd2af7274853ff91d6cd62541191d9fbd10d , https://git.kernel.org/stable/c/924f788c906dccaca30acab86c7124371e1d6f2c	O-LIN-LINU-030924/1203

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[10.017908] Workqueue: events_unbound padata_mt_helper [10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 : [10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330 [10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30 [10.018147] </TASK> Looking at the padata_mt_helper() function, the only way a divide-by-0 panic can happen is when ps-		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>chunk_size is 0. The way that chunk_size is initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least 1 no matter what the input parameters are. **CVE ID: CVE-2024-43889**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference in apply_state_adjust_rules Check the pointer value to fix potential null pointer dereference	https://git.kernel.org/stable/c/0c065e50445aea2e0a1815f12e97ee49e02cbaac, https://git.kernel.org/stable/c/13937a40aae4efe64592ba48c057ac3c72f7fe82, https://git.kernel.org/stable/c/3a01bf2ca9f860fdc88c358567b8fa3033efcf30	O-LIN-LINU-030924/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43907		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer dereference to ras_manager Check ras_manager before using it **CVE ID: CVE-2024-43908**	https://git.kernel.org/stable/c/033187a70ba9743c73a810a006816e5553d1e7d4, https://git.kernel.org/stable/c/48cada0ac79e4775236d642e9ec5998a7c7fb7a4, https://git.kernel.org/stable/c/4c11d30c95576937c6c35e6f29884761f2dddb43	O-LIN-LINU-030924/1205
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener	https://git.kernel.org/stable/c/05e4a0fa248240efd99a539853e844f0f0a9e6a5, https://git.kernel.org/stable/c/1407be30fc17eff918a98e0a990c0e988f11dc84, https://git.kernel.org/stable/c/52319d9d2f522ed939af31af70f8c3a0f0f67e6c	O-LIN-LINU-030924/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_sock() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint(). [0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89 f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DR7: 00000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI:		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0 R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated--- **CVE ID: CVE-2024-44935**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.26					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/cma: Do not change route.addr.src_addr outside state checks If the state is not idle then resolve_prepare_src() should immediately fail and no change to global state	https://git.kernel.org/stable/c/00265efbd3e5705038c9492a434fda8cf960c8a2, https://git.kernel.org/stable/c/22e9f71072fa605cbf033158db58e0790101928d, https://git.kernel.org/stable/c/5b1cef5798b4fd6e4fd5522e7b8a26248beeacaa	O-LIN-LINU-030924/1207

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should happen. However, it unconditionally overwrites the src_addr trying to build a temporary any address. For instance if the state is already RDMA_CM_LISTEN then this will corrupt the src_addr and would cause the test in cma_cancel_operation(): if (cma_any_addr(cma_src_addr(id_priv)) && !id_priv->cma_dev) Which would manifest as this trace from syzkaller: BUG: KASAN: use-after-free in __list_add_valid+0x93/0xa0 lib/list_debug.c:26 Read of size 8 at addr ffff8881546491e0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by task syz-executor.1/32204 CPU: 1 PID: 32204 Comm: syz-executor.1 Not tainted 5.12.0-rc8-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: __dump_stack lib/dump_stack.c:79 [inline] dump_stack+0x141/0x1d7 lib/dump_stack.c:120 print_address_description.constprop.0.cold+0x5b/0x2f8 mm/kasan/report.c:232 __kasan_report mm/kasan/report.c:399 [inline] kasan_report.cold+0x7c/0xd8 mm/kasan/report.c:416 __list_add_valid+0x		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	93/0xa0 lib/list_debug.c:26 __list_add include/linux/list.h:67 [inline] list_add_tail include/linux/list.h:100 [inline] cma_listen_on_all drivers/infiniband/core/cma.c:2557 [inline] rdma_listen+0x787/0xe00 drivers/infiniband/core/cma.c:3751 ucma_listen+0x16a/0x210 drivers/infiniband/core/ucma.c:1102 ucma_write+0x259/0x350 drivers/infiniband/core/ucma.c:1732 vfs_write+0x28e/0xa30 fs/read_write.c:603 ksys_write+0x1ee/0x250 fs/read_write.c:658 do_syscall_64+0x2d/0x70		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x44/0xae This is indicating that an rdma_id_private was destroyed without doing cma_cancel_listens(). Instead of trying to re-use the src_addr memory to indirectly create an any address derived from the dst build one explicitly on the stack and bind to that as any other normal flow would do. rdma_bind_addr() will copy it over the src_addr once it knows the state is valid. This is similar to commit bc0bdc5afaa7 ("RDMA/cma: Do not change route.addr.src_addr.ss_family")		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48925		
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption. next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80.	https://git.kernel.org/stable/c/33222d1571d7ce8c1c75f6b488f38968fa93d2d9, https://git.kernel.org/stable/c/4ce247af3f30078d5b97554f1ae6200a0222c15a, https://git.kernel.org/stable/c/669c2b178956718407af5631ccbc61c24413f038	O-LIN-LINU-030924/1208

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(next=ffffff80651764d0). [361.904380] [1:irq/191-dwc3:16979] Call trace: [361.904391] [1:irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1:irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1:irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1:irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4 [361.904426] [1:irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1:irq/191-dwc3:16979] dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1:irq/191-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c **CVE ID: CVE-2022-48926**		
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: make apf token non-zero to fix bug In current async pagefault logic, when a page is ready, KVM relies on kvm_arch_can_dequeue_async_page_present() to determine whether to deliver	https://git.kernel.org/stable/c/4c3644b6c96c5daa5149e5abddc07234eea47c7c, https://git.kernel.org/stable/c/62040f5cd7d937de547836e747b6aa8212fec573, https://git.kernel.org/stable/c/6f3c1fc53d86d580d8d6d749c4af23705e4f6f79	O-LIN-LINU-030924/1209

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	a READY event to the Guest. This function test token value of struct kvm_vcpu_pv_apf_data, which must be reset to zero by Guest kernel when a READY event is finished by Guest. If value is zero meaning that a READY event is done, so the KVM can deliver another. But the kvm_arch_setup_async_pf() may produce a valid token with zero value, which is confused with previous mention and may lead the loss of this READY event. This bug may cause task blocked forever in Guest: INFO: task stress:7532 blocked for more than 1254 seconds. Not tainted 5.10.0 #16 "echo 0 > /proc/sys/kernel/		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hung_task_timeout_secs" disables this message. task:stress state:D stack: 0 pid: 7532 ppid: 1409 flags:0x00000080 Call Trace: __schedule+0x1e7/0x650 schedule+0x46/0xb0 kvm_async_pf_task_wait_schedule+0xad/0xe0 ? exit_to_user_mode_prepare+0x60/0x70 __kvm_handle_async_pf+0x4f/0xb0 ? asm_exc_page_fault+0x8/0x30 exc_page_fault+0x6f/0x110 ? asm_exc_page_fault+0x8/0x30 asm_exc_page_fault+0x1e/0x30		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0033:0x402d00 RSP: 002b:00007ffd31912500 EFLAGS: 00010206 RAX: 0000000000071000 RBX: ffffffffffffffff RCX: 00000000021a32b0 RDX: 000000000007d011 RSI: 000000000007d000 RDI: 00000000021262b0 RBP: 00000000021262b0 R08: 0000000000000003 R09: 0000000000000086 R10: 00000000000000eb R11: 00007fefbdf2baa0 R12: 0000000000000000 R13: 0000000000000002 R14: 000000000007d000 R15: 0000000000001000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48943		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: fix memory leak in int3400_notify() It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies 4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65 NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b a5 rmal.kkkkkkkkkk. backtrace: [<ffffffff9c502c3e>]	https://git.kernel.org/stable/c/2e798814e01827871938ff172d2b2ccf1e74b355, https://git.kernel.org/stable/c/33c73a4d7e7b19313a6b417152f5365016926418, https://git.kernel.org/stable/c/3abea10e6a8f0e7804ed4c124bea2d15aca977c8	O-LIN-LINU-030924/1210

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	__kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0 [<ffffffff9c7b7d6e>] kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>] acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0 [<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0 [<ffffffff9c2cb4dd>] kthread+0xfd/0x130		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly. **CVE ID: CVE-2022-48924**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function. **CVE ID: CVE-2022-48928**	https://git.kernel.org/stable/c/0f88722313645a903f4d420ba61ddc690ec2481d, https://git.kernel.org/stable/c/1aa12ecfdcbafebc218910ec47acf6262e600cf5, https://git.kernel.org/stable/c/53d43a9c8dd224e66559fe86af1e473802c7130e	O-LIN-LINU-030924/1211
Improper Locking	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/081bdc9fe05bb23248f5effb6f811da3da4b8252,	O-LIN-LINU-030924/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync() **CVE ID: CVE-2022-48930**	https://git.kernel.org/stable/c/4752fafb461821f8c8581090c923ababba68c5bd, https://git.kernel.org/stable/c/8cc342508f9e7fdccd2e9758ae9d52aff72dab7f	
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix memory leak during stateful obj update stateful objects can be updated from the control plane. The transaction logic allocates a temporary object for this purpose. The ->init function was called for this object, so plain kfree() leaks resources. We must call ->destroy	https://git.kernel.org/stable/c/34bb90e407e3288f610558beaae54ecaa32b11c4, https://git.kernel.org/stable/c/53026346a94c43f35c32b18804041bc483271d87, https://git.kernel.org/stable/c/7e9880e81d3fd6a43c202f2057174852904328 26	O-LIN-LINU-030924/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the object. nft_obj_destroy does this, but it also decrements the module refcount, but the update path doesn't increment it. To avoid special-casing the update object release, do module_get for the update case too and release it via nft_obj_destroy(). **CVE ID: CVE-2022-48933**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: flower: Fix a potential leak in nfp_tunnel_add_shared_mac() ida_simple_get() returns an id between min (0) and max (NFP_MAX_MAC_INDEX) inclusive. So NFP_MAX_MAC_IN	https://git.kernel.org/stable/c/3a14d0888eb4b0045884126acc69abfb7b87814d, https://git.kernel.org/stable/c/4086d2433576baf85f0e538511df97c8101e0a10, https://git.kernel.org/stable/c/5ad5886f85b6bd893e3ed19013765fb0c243c069	O-LIN-LINU-030924/1214

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DEX (0xff) is a valid id. In order for the error handling path to work correctly, the 'invalid' value for 'ida_idx' should not be in the 0..NFP_MAX_MAC_INDEX range, inclusive. So set it to -1. **CVE ID: CVE-2022-48934**		
Use After Free	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unregister flowtable hooks on netns exit Unregister flowtable hooks before they are releases via nf_tables_flowtable_destroy() otherwise hook core reports UAF. BUG: KASAN: use-after-free in nf_hook_entries_grow+0x5a7/0x700	https://git.kernel.org/stable/c/6069da443bf65f513bb507bb21e2f87cfb1ad0b6, https://git.kernel.org/stable/c/88c795491bf45a8c08a0f94c9ca4f13722e51013, https://git.kernel.org/stable/c/8ffb8ac3448845f65634889b051bd65e4dee484b	O-LIN-LINU-030924/1215

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/core.c:142 net/netfilter/core.c:142 Read of size 4 at addr ffff8880736f7438 by task syz-executor579/3666 CPU: 0 PID: 3666 Comm: syz-executor579 Not tainted 5.16.0-rc5-syzkaller #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 lib/dump_stack.c:88 [inline] lib/dump_stack.c:106 dump_stack_lvl+0x1dc/0x2d8 lib/dump_stack.c:106 lib/dump_stack.c:106 print_address_desc		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ription+0x65/0x380 mm/kasan/report.c:247 mm/kasan/report.c:247 __kasan_report mm/kasan/report.c:433 [inline] __kasan_report mm/kasan/report.c:433 [inline] mm/kasan/report.c:450 kasan_report+0x19a/0x1f0 mm/kasan/report.c:450 mm/kasan/report.c:450 nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 __nf_register_net_hook+0x27e/0x8d0 net/netfilter/core.c:429 net/netfilter/core.c:429 nf_register_net_hook+0xaa/0x180 net/netfilter/core.c:571 net/netfilter/core.c:571		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nft_register_flowtable_net_hooks+0x3c5/0x730 net/netfilter/nf_tables_api.c:7232 net/netfilter/nf_tables_api.c:7232 nf_tables_newflowtable+0x2022/0x2cf0 net/netfilter/nf_tables_api.c:7430 net/netfilter/nf_tables_api.c:7430 nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv+0x10e6/0x2550 net/netfilter/nfnetl		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ink.c:652 net/netfilter/nfnetlink.c:652 __nft_release_hook() calls nft_unregister_flowtable_net_hooks() which only unregisters the hooks, then after RCU grace period, it is guaranteed that no packets add new entries to the flowtable (no flow offload rules and flowtable hooks are reachable from packet path), so it is safe to call nf_flow_table_free() which cleans up the remaining entries from the flowtable (both software and hardware) and it unbinds the flow_block. **CVE ID: CVE-2022-48935**		
Integer Overflow or Wraparound	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/49909c9f8458cacb5b241106cba65aba5a6d8f4c, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CDC-NCM: avoid overflow in sanity checking A broken device may give an extreme offset like 0xFFF0 and a reasonable length for a fragment. In the sanity check as formulated now, this will create an integer overflow, defeating the sanity check. Both offset and offset + len need to be checked in such a manner that no overflow can occur. And those quantities should be unsigned. **CVE ID: CVE-2022-48938**	69560efa001397ebb8dc1c3e6a3ce00302bb9f7f, https://git.kernel.org/stable/c/7b737e47b87589031f0d4657f6d7b0b770474925	
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: hwmon: Handle failure to register sensor with thermal zone correctly	https://git.kernel.org/stable/c/1b5f517cca36292076d9e38fa6e33a257703e62e, https://git.kernel.org/stable/c/7efe8499cb90651c540753f4269d2d43ede14223,	O-LIN-LINU-030924/1217

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If an attempt is made to a sensor with a thermal zone and it fails, the call to devm_thermal_zone_of_sensor_register() may return -ENODEV. This may result in crashes similar to the following. Unable to handle kernel NULL pointer dereference at virtual address 00000000000003cd ... Internal error: Oops: 96000021 [#1] PREEMPT SMP ... pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : mutex_lock+0x18/0x60 lr : thermal_zone_device_update+0x40/0x2e0 sp : ffff800014c4fc60	https://git.kernel.org/stable/c/8a1969e14ad93663f9a3ed02ccc2138da9956a0e	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x29: ffff800014c4fc60 x28: ffff365ee3f6e000 x27: ffffdde218426790 x26: ffff365ee3f6e000 x25: 0000000000000000 x24: ffff365ee3f6e000 x23: ffffdde218426870 x22: ffff365ee3f6e000 x21: 00000000000003cd x20: ffff365ee8bf3308 x19: ffffffffffffffed x18: 0000000000000000 x17: ffffdde21842689c x16: ffffdde1cb7a0b7c x15: 0000000000000040 x14: ffffdde21a4889a0 x13: 0000000000000228 x12: 0000000000000000 x11: 0000000000000000 x10:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 x9 : 0000000000000000 x8 : 0000000001120000 x7 : 0000000000000001 x6 : 0000000000000000 x5 : 0068000878e20f07 x4 : 0000000000000000 x3 : 00000000000003cd x2 : ffff365ee3f6e000 x1 : 0000000000000000 x0 : 00000000000003cd Call trace: mutex_lock+0x18/0x60 hwmon_notify_event+0xfc/0x110 0xffffdde1cb7a0a90 0xffffdde1cb7a0b7c irq_thread_fn+0x2c/0xa0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			irq_thread+0x134/0x240 kthread+0x178/0x190 ret_from_fork+0x10/0x20 Code: d503201f d503201f d2800001 aa0103e4 (c8e47c02) Jon Hunter reports that the exact call sequence is: hwmon_notify_event() --> hwmon_thermal_notify() --> thermal_zone_device_update() --> update_temperature() --> mutex_lock() The hwmon core needs to handle all errors returned from calls to devm_thermal_zon		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			e_of_sensor_register(). If the call fails with -ENODEV, report that the sensor was not attached to a thermal zone but continue to register the hwmon device. **CVE ID: CVE-2022-48942**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is:	https://git.kernel.org/stable/c/3aadfd46858b1f64d4d6a0654b863e21aabff975, https://git.kernel.org/stable/c/40805099af11f68c5ca7dbcfacf455da8f99f622, https://git.kernel.org/stable/c/84ec758fb2daa236026506868c8796b0500c047d	O-LIN-LINU-030924/1218

<table>
<tr><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description &amp; CVE ID</th><th>Patch</th><th>NCIIPC ID</th></tr>
<tr><td></td><td></td><td></td><td>A --> B --> C --> D
A <-- B <-- C <-- D
delete list_head *B | delete list_head *C
-------------------------------|-----------------------------------
configfs_unregister_subsystem | configfs_unregister_subsystem
unlink_group | unlink_group
unlink_obj | unlink_obj
list_del_init | list_del_init
__list_del_entry | __list_del_entry
__list_del | __list_del
// next == C |
next->prev = prev |
| next->prev = prev
prev->next = next |
| // prev == B
| prev->next = next</td><td></td><td></td></tr>
</table>

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix this by adding mutex when calling link_group() or unlink_group(), but parent configfs_subsystem is NULL when config_item is root. So I create a mutex configfs_subsystem_mutex. **CVE ID: CVE-2022-48931**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: ice: fix concurrent reset and removal of VFs Commit c503e63200c6 ("ice: Stop processing VF messages during teardown") introduced a driver state flag, ICE_VF_DEINIT_IN_PROGRESS, which is intended to prevent some issues with concurrently handling messages from VFs while tearing down the VFs.	https://git.kernel.org/stable/c/05ae1f0fe9c6c5ead08b306e665763a352d20716, https://git.kernel.org/stable/c/2a3e61de89bab6696aa28b70030eb119968c5586, https://git.kernel.org/stable/c/3c805fce07c9dbc47d8a9129c7c5458025951957	O-LIN-LINU-030924/1219

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This change was motivated by crashes caused while tearing down and bringing up VFs in rapid succession. It turns out that the fix actually introduces issues with the VF driver caused because the PF no longer responds to any messages sent by the VF during its .remove routine. This results in the VF potentially removing its DMA memory before the PF has shut down the device queues. Additionally, the fix doesn't actually resolve concurrency issues within the ice driver. It is possible for a VF to initiate a reset just prior to the ice driver removing VFs. This		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can result in the remove task concurrently operating while the VF is being reset. This results in similar memory corruption and panics purportedly fixed by that commit. Fix this concurrency at its root by protecting both the reset and removal flows using the existing VF cfg_lock. This ensures that we cannot remove the VF while any outstanding critical tasks such as a virtchnl message or a reset are occurring. This locking change also fixes the root cause originally fixed by commit c503e63200c6 ("ice: Stop processing VF messages during teardown"), so we can simply revert it.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note that I kept these two changes together because simply reverting the original commit alone would leave the driver vulnerable to worse race conditions. **CVE ID: CVE-2022-48941**		
Improper Locking	22-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: io_uring: add a schedule point in io_add_buffers() Looping ~65535 times doing kmalloc() calls can trigger soft lockups, especially with DEBUG features (like KASAN). [253.536212] watchdog: BUG: soft lockup - CPU#64 stuck for 26s! [b219417889:12575] [253.544433] Modules linked in: vfat fat	https://git.kernel.org/stable/c/4a93c6594613c3429b6f30136fff115c7f803af4, https://git.kernel.org/stable/c/8f3cc3c5bc43d03b5748ac4fb8d180084952c36a, https://git.kernel.org/stable/c/c718ea4e7382e18957ed0e88a5f855e2122d9c00	O-LIN-LINU-030924/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			i2c_mux_pca954x i2c_mux spidev cdc_acm xhci_pci xhci_hcd sha3_generic gq(O) [253.544451] CPU: 64 PID: 12575 Comm: b219417889 Tainted: G S O 5.17.0-smp-DEV #801 [253.544457] RIP: 0010:kernel_text_address (./include/asm-generic/sections.h:192 ./include/linux/kallsyms.h:29 kernel/extable.c:67 kernel/extable.c:98) [253.544464] Code: 0f 93 c0 48 c7 c1 e0 63 d7 a4 48 39 cb 0f 92 c1 20 c1 0f b6 c1 5b 5d c3 90 0f 1f 44 00 00 55 48 89 e5 41 57 41 56 53 48 89 fb <48> c7 c0 00 00 80 a0 41 be 01 00 00 00 48 39 c7 72 0c 48 c7 c0 40 [253.544468] RSP: 0018:ffff8882d8baf4c0 EFLAGS: 00000246 [253.544471] RAX: 1ffff1105b175e00		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBX: ffffffffa13ef09a RCX: 00000000a13ef001 [253.544474] RDX: ffffffffa13ef09a RSI: ffff8882d8baf558 RDI: ffffffffa13ef09a [253.544476] RBP: ffff8882d8baf4d8 R08: ffff8882d8baf5e0 R09: 0000000000000004 [253.544479] R10: ffff8882d8baf5e8 R11: ffffffffa0d59a50 R12: ffff8882eab20380 [253.544481] R13: ffffffffa0d59a50 R14: dffffc0000000000 R15: 1ffff1105b175eb0 [253.544483] FS: 00000000016d3380(0000) GS:ffff88af48c00000(0000) knlGS:0000000000000000 [253.544486] CS: 0010 DS: 0000 ES: 0000 CR0:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000080050033 [253.544488] CR2: 00000000004af0f0 CR3: 00000002eabfa004 CR4: 00000000003706e0 [253.544491] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [253.544492] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [253.544494] Call Trace: [253.544496] <TASK> [253.544498] ? io_queue_sqe (fs/io_uring.c:7143) [253.544505] __kernel_text_address (kernel/extable.c:78) [253.544508] unwind_get_return_address		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(arch/x86/kernel/unwind_frame.c:19) [253.544514] arch_stack_walk (arch/x86/kernel/stacktrace.c:27) [253.544517] ? io_queue_sqe (fs/io_uring.c:7143) [253.544521] stack_trace_save (kernel/stacktrace.c:123) [253.544527] ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544531] ? ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544533] ? __kasan_kmalloc (mm/kasan/common.c:524) [253.544535] ? kmem_cache_alloc_trace		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(./include/linux/kasan.h:270 mm/slab.c:3567) [253.544541] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544544] ? __io_queue_sqe (fs/io_uring.c:?) [253.544551] __kasan_kmalloc (mm/kasan/common.c:524) [253.544553] kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544556] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544560] io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544564] ? __kasan_slab_alloc (mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544567] ? __kasan_slab_alloc		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544569] ? kmem_cache_alloc_bulk (mm/slab.h:732 mm/slab.c:3546) [253.544573] ? __io_alloc_req_refill (fs/io_uring.c:2078) [253.544578] ? io_submit_sqes (fs/io_uring.c:7441) [253.544581] ? __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uring.c:10096) [253.544584] ? __x64_sys_io_uring_enter (fs/io_uring.c:10096) [253.544587] ? do_syscall_64 (arch/x86/entry/common.c:50 arch/x86/entry/common.c:80) [253.544590] ? entry_SYSCALL_64_		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after_hwframe (??:?) [253.544596] __io_queue_sqe (fs/io_uring.c:?) [253.544600] io_queue_sqe (fs/io_uring.c:7143) [253.544603] io_submit_sqe (fs/io_uring.c:?) [253.544608] io_submit_sqes (fs/io_uring.c:?) [253.544612] __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uri ---truncated--- **CVE ID: CVE-2022-48937**		
Excessive Iteration	22-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: bpf: Add schedule points in batch ops syzbot reported various soft lockups caused by bpf batch operations. INFO: task kworker/1:1:27	https://git.kernel.org/stable/c/75134f16e7dd0007aa474b281935c5f42e79f2c8, https://git.kernel.org/stable/c/7e8099967d0e3ff9d1ae043e80b27fbe46c08417, https://git.kernel.org/stable/c/7ef94bfb08fb9e73defafbd5ddef6b5a0e2ee12b	O-LIN-LINU-030924/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blocked for more than 140 seconds. INFO: task hung in rcu_barrier Nothing prevents batch ops to process huge amount of data, we need to add schedule points in them. Note that maybe_wait_bpf_programs(map) calls from generic_map_delete_batch() can be factorized by moving the call after the loop. This will be done later in -next tree once we get this fix merged, unless there is strong opinion doing this optimization sooner. **CVE ID: CVE-2022-48939**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.27					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/05f7927b25d26	O-LIN-LINU-030924/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	vulnerability has been resolved: netfilter: fix use-after-free in __nf_register_net_hook() We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430	35e87267ff6c79db79fb46cf313, https://git.kernel.org/stable/c/49c24579cec41e32f13d57b337fd28fb208d4a5b, https://git.kernel.org/stable/c/56763f12b0f02706576a088e85ef856deacc98a0	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #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+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 nf_hook_entries_get_hook_ops		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218 synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0 net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101 ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084 __sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockop		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			t net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xba/0x150 net/socket.c:2188 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: 0033:0x7f65a1ace7d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 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 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9 RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12: 00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000 </TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000 (node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x35a/0x4a0 mm/slub. ---truncated--- **CVE ID: CVE-2022-48912**		
Double Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root()	https://git.kernel.org/stable/c/147a0e71ccf96df9fc8c2ac500829d8e423ef02c, https://git.kernel.org/stable/c/2fe0e281f7ad0a62259649764228227dd6b2561d,	O-LIN-LINU-030924/1223

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4	https://git.kernel.org/stable/c/3d6cc9898efdfb062efb74dc18cfc700e082f5d5	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae **CVE ID: CVE-2022-48919**		
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: core: Fix TZ_GET_TRIP NULL pointer dereference Do not call get_trip_hyst() from thermal_genl_cmd_tz_get_trip() if the thermal zone does not define one. **CVE ID: CVE-2022-48915**	https://git.kernel.org/stable/c/1c0b51e62a50e9291764d022ed44549e65d6ab9c, https://git.kernel.org/stable/c/3dafbf915c05f83469e791949b5590da2aca2afb, https://git.kernel.org/stable/c/4c294285cec3964b3291772ac0642c2bf440bd1b	O-LIN-LINU-030924/1224
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.89					
NULL Pointer Dereference	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: efi: fix NULL-deref in init error path In cases where runtime services	https://git.kernel.org/stable/c/4ca71bc0e1995d15486cd7b60845602a28399cb5, https://git.kernel.org/stable/c/585a0b2b3ae7903c6abee3087d09c69e955a779	O-LIN-LINU-030924/1225

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are not supported or have been disabled, the runtime services workqueue will never have been allocated. Do not try to destroy the workqueue unconditionally in the unlikely event that EFI initialisation fails to avoid dereferencing a NULL pointer. **CVE ID: CVE-2022-48879**	4, https://git.kernel.org/stable/c/5fcf75a8a4c3e7ee9122d143684083c9faf20452	
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.90					
Use After Free	21-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_qca: Fix driver shutdown on closed serdev The driver shutdown callback (which sends EDL_SOC_RESET to the device over serdev) should not be	https://git.kernel.org/stable/c/272970be3dabd24cbe50e393ffee8f04aec3b9a8, https://git.kernel.org/stable/c/908d1742b6e694e84ead5c62e4b7c1bfbb8b46a3, https://git.kernel.org/stable/c/e84ec6e25df9bb0968599e92eacedaf3a0a5b587	O-LIN-LINU-030924/1226

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoked when HCI device is not open (e.g. if hci_dev_open_sync() failed), because the serdev and its TTY are not open either. Also skip this step if device is powered off (qca_power_shutdown()). The shutdown callback causes use-after-free during system reboot with Qualcomm Atheros Bluetooth: Unable to handle kernel paging request at virtual address 0072662f67726fd7 ... CPU: 6 PID: 1 Comm: systemd-shutdow Tainted: G W 6.1.0-rt5-00325-g8a5f56bcfcca #8 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tty_driver_flush_buffer+0x4/0x30 serdev_device_write_flush+0x24/0x34 qca_serdev_shutdown+0x80/0x130 [hci_uart] device_shutdown+0x15c/0x260 kernel_restart+0x48/0xac KASAN report: BUG: KASAN: use-after-free in tty_driver_flush_buffer+0x1c/0x50 Read of size 8 at addr ffff16270c2e0018 by task systemd-shutdow/1 CPU: 7 PID: 1 Comm: systemd-shutdow Not tainted 6.1.0-next-20221220-00014-gb85aaf97fb01-dirty #28 Hardware name: Qualcomm		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	Technologies, Inc. Robotics RB5 (DT) Call trace: dump_backtrace.part.0+0xdc/0xf0 show_stack+0x18/0x30 dump_stack_lvl+0x68/0x84 print_report+0x188/0x488 kasan_report+0xa4/0xf0 __asan_load8+0x80/0xac tty_driver_flush_buffer+0x1c/0x50 ttyport_write_flush+0x34/0x44 serdev_device_write_flush+0x48/0x60 qca_serdev_shutdown+0x124/0x274 device_shutdown+0x1e8/0x350 kernel_restart+0x48/0xb0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__do_sys_reboot+0x244/0x2d0 __arm64_sys_reboot+0x54/0x70 invoke_syscall+0x60/0x190 el0_svc_common.constprop.0+0x7c/0x160 do_el0_svc+0x44/0xf0 el0_svc+0x2c/0x6c el0t_64_sync_handler+0xbc/0x140 el0t_64_sync+0x190/0x194 **CVE ID: CVE-2022-48878**		
Affected Version(s): From (including) 5.12 Up to (excluding) 5.15.27					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: blktrace: fix use after free for struct blk_trace When tracing the whole disk,	https://git.kernel.org/stable/c/30939293262eb433c960c4532a0d59c4073b2b84, https://git.kernel.org/stable/c/6418634238ade86f2b08192928787f39d8afb58c, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	'dropped' and 'msg' will be created under 'q->debugfs_dir' and 'bt->dir' is NULL, thus blk_trace_free() won't remove those files. What's worse, the following UAF can be triggered because of accessing stale 'dropped' and 'msg': == BUG: KASAN: use-after-free in blk_dropped_read+0x89/0x100 Read of size 4 at addr ffff88816912f3d8 by task blktrace/1188 CPU: 27 PID: 1188 Comm: blktrace Not tainted 5.17.0-rc4-next-20220217+ #469 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ?-	78acc7dbd84a8c173a08584750845c31611160f2	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20190727_073836-4 Call Trace: <TASK> dump_stack_lvl+0x34/0x44 print_address_description.constprop.0.cold+0xab/0x381 ? blk_dropped_read+0x89/0x100 ? blk_dropped_read+0x89/0x100 kasan_report.cold+0x83/0xdf ? blk_dropped_read+0x89/0x100 kasan_check_range+0x140/0x1b0 blk_dropped_read+0x89/0x100 ? blk_create_buf_file_callback+0x20/0x20 ? kmem_cache_free+0xa1/0x500 ? do_sys_openat2+0x258/0x460		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			full_proxy_read+0x8f/0xc0 vfs_read+0xc6/0x260 ksys_read+0xb9/0x150 ? vfs_write+0x3d0/0x3d0 ? fpregs_assert_state_consistent+0x55/0x60 ? exit_to_user_mode_prepare+0x39/0x1e0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fbc080d92fd Code: ce 20 00 00 75 10 b8 00 00 00 00 0f 05 48 3d 01 f0 ff ff 73 31 c3 48 83 1 RSP: 002b:00007fbb95ff9cb0 EFLAGS: 00000293 ORIG_RAX:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 RAX: ffffffffffffffda RBX: 00007fbb95ff9dc0 RCX: 00007fbc080d92fd RDX: 0000000000000100 RSI: 00007fbb95ff9cc0 RDI: 0000000000000045 RBP: 0000000000000045 R08: 0000000000406299 R09: 00000000fffffffd R10: 000000000153afa0 R11: 0000000000000293 R12: 00007fbb780008c0 R13: 00007fbb78000938 R14: 0000000000608b30 R15: 00007fbb780029c8 </TASK> Allocated by task 1050: kasan_save_stack+0x1e/0x40		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kasan_kmalloc+0x81/0xa0 do_blk_trace_setup+0xcb/0x410 __blk_trace_setup+0xac/0x130 blk_trace_ioctl+0xe9/0x1c0 blkdev_ioctl+0xf1/0x390 __x64_sys_ioctl+0xa5/0xe0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae Freed by task 1050: kasan_save_stack+0x1e/0x40 kasan_set_track+0x21/0x30 kasan_set_free_info+0x20/0x30 __kasan_slab_free+0x103/0x180		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	kfree+0x9a/0x4c0 __blk_trace_remove+0x53/0x70 blk_trace_ioctl+0x199/0x1c0 blkdev_common_ioctl+0x5e9/0xb30 blkdev_ioctl+0x1a5/0x390 __x64_sys_ioctl+0xa5/0xe0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae The buggy address belongs to the object at ffff88816912f380 which belongs to the cache kmalloc-96 of size 96 The buggy address is located 88 bytes inside of 96-byte region [ffff88816912f380, ffff88816912f3e0) The buggy address belongs to the page:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page:000000009a1b4e7c refcount:1 mapcount:0 mapping:0000000000000000 index:0x0f flags: 0x17ffffc0000200(slab|node=0|zone=2|lastcpupid=0x1fffff) raw: 0017ffffc0000200 ffffea00044f1100 dead000000000002 ffff88810004c780 raw: 0000000000000000 0000000000200020 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff88816912f280: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f300: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc >ffff88816912f380: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			^ ffff88816912f400: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f480: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc == **CVE ID: CVE-2022-48913**		
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iwlwifi: mvm: check debugfs_dir ptr before use When "debugfs=off" is used on the kernel command line, iwiwifi's mvm module uses an invalid/unchecked debugfs_dir pointer and causes a BUG: BUG: kernel NULL pointer dereference, address:	https://git.kernel.org/stable/c/5a6248c0a22352f09ea041665d3bd3e18f6f872c, https://git.kernel.org/stable/c/7de1ed755e1ace30d97a724bad32452ed86b653b, https://git.kernel.org/stable/c/fe51975ff13831e794e1bcd0039b305dcad3d7ba	O-LIN-LINU-030924/1228

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			000000000000004f #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP CPU: 1 PID: 503 Comm: modprobe Tainted: G W 5.17.0-rc5 #7 Hardware name: Dell Inc. Inspiron 15 5510/076F7Y, BIOS 2.4.1 11/05/2021 RIP: 0010:iwl_mvm_dbgfs_register+0x692/0x700 [iwlmvm] Code: 69 a0 be 80 01 00 00 48 c7 c7 50 73 6a a0 e8 95 cf ee e0 48 8b 83 b0 1e 00 00 48 c7 c2 54 73 6a a0 be 64 00 00 00 48 8d 7d 8c <48> 8b 48 50 e8 15 22 07 e1 48 8b 43 28 48 8d 55 8c 48 c7 c7 5f 73 RSP: 0018:ffffc90000a0ba68 EFLAGS: 00010246 RAX: ffffffffffffffff RBX:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff88817d6e3328 RCX: ffff88817d6e3328 RDX: ffffffffa06a7354 RSI: 0000000000000064 RDI: ffffc90000a0ba6c RBP: ffffc90000a0bae0 R08: ffffffff824e4880 R09: ffffffffa069d620 R10: ffffc90000a0ba00 R11: ffffffffffffffff R12: 0000000000000000 R13: ffffc90000a0bb28 R14: ffff88817d6e3328 R15: ffff88817d6e3320 FS: 00007f64dd92d740(0000) GS:ffff88847f640000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004f CR3: 000000016fc7900		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1 CR4: 0000000000770ee0 PKRU: 55555554 Call Trace: <TASK> ? iwl_mvm_mac_setup_register+0xbdc/0xda0 [iwlmvm] iwl_mvm_start_post_nvm+0x71/0x100 [iwlmvm] iwl_op_mode_mvm_start+0xab8/0xb30 [iwlmvm] _iwl_op_mode_start+0x6f/0xd0 [iwlwifi] iwl_opmode_register+0x6a/0xe0 [iwlwifi] ? 0xffffffffa0231000 iwl_mvm_init+0x35/0x1000 [iwlmvm] ? 0xffffffffa0231000 do_one_initcall+0x5a/0x1b0 ? kmem_cache_alloc+0x1e5/0x2f0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_init_module+0x1e/0x220 do_init_module+0x48/0x220 load_module+0x2602/0x2bc0 ? __kernel_read+0x145/0x2e0 ? kernel_read_file+0x229/0x290 __do_sys_finit_module+0xc5/0x130 ? __do_sys_finit_module+0xc5/0x130 __x64_sys_finit_module+0x13/0x20 do_syscall_64+0x38/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f64dda564dd Code: 5b 41 5c c3 66 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 1b 29 0f 00 f7 d8 64 89 01 48 RSP: 002b:00007ffdba393f88 EFLAGS: 00000246 ORIG_RAX: 0000000000000139 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f64dda564dd RDX: 0000000000000000 RSI: 00005575399e2ab2 RDI: 0000000000000001 RBP: 000055753a91c5e0 R08: 0000000000000000 R09: 0000000000000002 R10: 0000000000000001 R11: 0000000000000246 R12: 00005575399e2ab2 R13: 000055753a91ceb0 R14:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 R15: 000055753a923018 </TASK> Modules linked in: btintel(+) btmtk bluetooth vfat snd_hda_codec_hdmi fat snd_hda_codec_realtek snd_hda_codec_generic iwlmvm(+) snd_sof_pci_intel_tgl mac80211 snd_sof_intel_hda_common soundwire_intel soundwire_generic_allocation soundwire_cadence soundwire_bus snd_sof_intel_hda snd_sof_pci snd_sof snd_sof_xtensa_dsp snd_soc_hdac_hda snd_hda_ext_core snd_soc_acpi_intel_match snd_soc_acpi snd_soc_core btrfs snd_compress snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec raid6_pq iwlwifi snd_hda_core snd_pcm snd_timer snd soundcore cfg80211 intel_ish_ipc(+) thunderbolt rfkill		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intel_ishtp ucsi_acpi wmi i2c_hid_acpi i2c_hid evdev CR2: 000000000000004f ---[end trace 0000000000000000]--- Check the debugfs_dir pointer for an error before using it. [change to make both conditional] **CVE ID: CVE-2022-48918**		
Affected Version(s): From (including) 5.14 Up to (excluding) 5.15.26					
Out-of-bounds Write	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: iio: adc: tsc2046: fix memory corruption by preventing array overflow On one side we have indio_dev->num_channels includes all physical channels + timestamp channel. On other side we	https://git.kernel.org/stable/c/082d2c047b0d305bb0b6e9f9d671a09470e2db2d, https://git.kernel.org/stable/c/0cb9b2f73c182d242a640e512f4785c7c504512f, https://git.kernel.org/stable/c/b7a78a8adaa8849c02f174d707aead0f85dca0da	O-LIN-LINU-030924/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have an array allocated only for physical channels. So, fix memory corruption by ARRAY_SIZE() instead of num_channels variable. Note the first case is a cleanup rather than a fix as the software timestamp channel bit in active_scanmask is never set by the IIO core. **CVE ID: CVE-2022-48927**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.26					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix crash due to incorrect copy_map_value When both bpf_spin_lock and bpf_timer are present in a BPF map value, copy_map_value needs to skirt both objects when	https://git.kernel.org/stable/c/719d1c2524c89ada78c4c9202641c1d9e942a322, https://git.kernel.org/stable/c/a8abb0c3dc1e28454851a00f8b7333d9695d566c, https://git.kernel.org/stable/c/eca9bd215d2233de79d930fa97aefbce03247a98	O-LIN-LINU-030924/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			copying a value into and out of the map. However, the current code does not set both s_off and t_off in copy_map_value, which leads to a crash when e.g. bpf_spin_lock is placed in map value with bpf_timer, as bpf_map_update_elem call will be able to overwrite the other timer object. When the issue is not fixed, an overwriting can produce the following splat: [root@(none) bpf]# ./test_progs -t timer_crash [15.930339] bpf_testmod: loading out-of-tree module taints kernel. [16.037849] ===		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			===================== [16.038458] BUG: KASAN: user-memory-access in __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.038944] Write of size 8 at addr 00000000000043ec0 by task test_progs/325 [16.039399] [16.039514] CPU: 0 PID: 325 Comm: test_progs Tainted: G OE 5.16.0+ #278 [16.039983] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ArchLinux 1.15.0-1 04/01/2014 [16.040485] Call Trace: [16.040645] <TASK> [16.040805] dump_stack_lvl+0x59/0x73 [16.041069] ? __pv_queued_spin_lock_slowpath+0x32b/0x520		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16.041427] kasan_report.cold+0x116/0x11b [16.041673] ? __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042040] __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042328] ? memcpy+0x39/0x60 [16.042552] ? pv_hash+0xd0/0xd0 [16.042785] ? lockdep_hardirqs_off+0x95/0xd0 [16.043079] __bpf_spin_lock_irqsave+0xdf/0xf0 [16.043366] ? bpf_get_current_comm+0x50/0x50 [16.043608] ? jhash+0x11a/0x270 [16.043848] bpf_timer_cancel+0x34/0xe0 [16.044119] bpf_prog_c4ea1c0f7449940d_sys_enter+0x7c/0x81 [16.044500] bpf_trampoline_6442477838_0+0x36/0x1000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16.044836] __x64_sys_nanosleep+0x5/0x140 [16.045119] do_syscall_64+0x59/0x80 [16.045377] ? lock_is_held_type+0xe4/0x140 [16.045670] ? irqentry_exit_to_user_mode+0xa/0x40 [16.046001] ? mark_held_locks+0x24/0x90 [16.046287] ? asm_exc_page_fault+0x1e/0x30 [16.046569] ? asm_exc_page_fault+0x8/0x30 [16.046851] ? lockdep_hardirqs_on+0x7e/0x100 [16.047137] entry_SYSCALL_64_after_hwframe+0x44/0xae [16.047405] RIP: 0033:0x7f9e4831718d [16.047602] Code: b4 0c 00 0f 05 eb a9 66 0f 1f 44 00 00 f3 0f 1e fa 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 8b 0d b3 6c 0c		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00 f7 d8 64 89 01 48 [16.048764] RSP: 002b:00007fff488086b8 EFLAGS: 00000206 ORIG_RAX: 0000000000000023 [16.049275] RAX: ffffffffffffffda RBX: 00007f9e48683740 RCX: 00007f9e4831718d [16.049747] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 00007fff488086d0 [16.050225] RBP: 00007fff488086f0 R08: 00007fff488085d7 R09: 00007f9e4cb594a0 [16.050648] R10: 0000000000000000 R11: 0000000000000206 R12: 00007f9e484cde30 [16.051124] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16.051608] </TASK> [16.051762] == **CVE ID: CVE-2022-48940**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.89					
Double Free	21-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: sched/core: Fix use-after-free bug in dup_user_cpus_ptr() Since commit 07ec77a1d4e8 ("sched: Allow task CPU affinity to be restricted on asymmetric systems"), the setting and clearing of user_cpus_ptr are done under pi_lock for arm64 architecture. However, dup_user_cpus_ptr() accesses user_cpus_ptr without any lock	https://git.kernel.org/stable/c/7b5cc7fd1789ea5dbb942c9f8207b076d365badc, https://git.kernel.org/stable/c/87ca4f9efbd7cc649ff43b87970888f2812945b8, https://git.kernel.org/stable/c/b22faa21b6230d5eccd233e1b7e0026a5002b287	O-LIN-LINU-030924/1231

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	protection. Since sched_setaffinity() can be invoked from another process, the process being modified may be undergoing fork() at the same time. When racing with the clearing of user_cpus_ptr in __set_cpus_allowed_ptr_locked(), it can lead to user-after-free and possibly double-free in arm64 kernel. Commit 8f9ea86fdf99 ("sched: Always preserve the user requested cpumask") fixes this problem as user_cpus_ptr, once set, will never be cleared in a task's lifetime. However, this bug was re-introduced in commit 851a723e45d1 ("sched: Always clear user_cpus_ptr in do_set_cpus_allowed()") which allows		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the clearing of user_cpus_ptr in do_set_cpus_allowed(). This time, it will affect all arches. Fix this bug by always clearing the user_cpus_ptr of the newly cloned/forked task before the copying process starts and check the user_cpus_ptr state of the source task under pi_lock. Note to stable, this patch won't be applicable to stable releases. Just copy the new dup_user_cpus_ptr() function over. **CVE ID: CVE-2022-48892**		
Affected Version(s): From (including) 5.15 Up to (excluding) 6.1.104					
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix potential null-ptr-deref in ip6table_nat_table_init().	https://git.kernel.org/stable/c/419ee6274c5153b89c4393c1946faa4c3cad4f9e, https://git.kernel.org/stable/c/87dba44e9471b79b255d0736858a897332db9226, https://git.kern	O-LIN-LINU-030924/1232

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip6table_nat_table_init() accesses net->gen->ptr[ip6table_nat_net_ops.id], but the function is exposed to user space before the entry is allocated via register_pernet_subsys(). Let's call register_pernet_subsys() before xt_register_template(). **CVE ID: CVE-2024-42269**	el.org/stable/c/91b6df6611b7edb28676c4f63f90c56c30d3e601	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix null-ptr-deref in iptable_nat_table_init(). We had a report that iptables-restore sometimes triggered null-ptr-deref at boot time. [0] The problem is that iptable_nat_table_i	https://git.kernel.org/stable/c/08ed888b69a22647153fe2bec55b7cd0a46102cc, https://git.kernel.org/stable/c/5830aa863981d43560748aa93589c0695191d95d, https://git.kernel.org/stable/c/70014b73d7539fcbb6b4ff5f37368d7241d8e626	O-LIN-LINU-030924/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	nit() is exposed to user space before the kernel fully initialises netns. In the small race window, a user could call iptable_nat_table_init() that accesses net_generic(net, iptable_nat_net_id), which is available only after registering iptable_nat_net_ops. Let's call register_pernet_subsys() before xt_register_template(). [0]: bpfilter: Loaded bpfilter_umh pid 11702 Started bpfilter BUG: kernel NULL pointer dereference, address: 0000000000000013		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PF: supervisor write access in kernel mode PF: error_code(0x0002) - not-present page PGD 0 P4D 0 PREEMPT SMP NOPTI CPU: 2 PID: 11879 Comm: iptables-restor Not tainted 6.1.92-99.174.amzn2023.x86_64 #1 Hardware name: Amazon EC2 c6i.4xlarge/, BIOS 1.0 10/16/2017 RIP: 0010:iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat Code: 10 4c 89 f6 48 89 ef e8 0b 19 bb ff 41 89 c4 85 c0 75 38 41 83 c7 01 49 83 c6 28 41 83 ff 04 75 dc 48 8b 44 24 08 48 8b 0c 24 <48> 89 08 4c 89 ef e8 a2 3b a2 cf 48 83 c4 10 44 89 e0 5b 5d 41 5c RSP: 0018:ffffbef902843		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cd0 EFLAGS: 00010246 RAX: 0000000000000013 RBX: ffff9f4b052caa20 RCX: ffff9f4b20988d80 RDX: 0000000000000000 RSI: 0000000000000064 RDI: ffffffffc04201c0 RBP: ffff9f4b29394000 R08: ffff9f4b07f77258 R09: ffff9f4b07f77240 R10: 0000000000000000 R11: ffff9f4b09635388 R12: 0000000000000000 R13: ffff9f4b1a3c6c00 R14: ffff9f4b20988e20 R15: 0000000000000004 FS: 00007f6284340000(0000) GS:ffff9f51fe280000(0000) knlGS:0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000013 CR3: 00000001d10a6005 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? xt_find_table_lock (net/netfilter/x_tables.c:1259) ? __die_body.cold (arch/x86/kernel/		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dumpstack.c:478 arch/x86/kernel/dumpstack.c:420) ? page_fault_oops (arch/x86/mm/fault.c:727) ? exc_page_fault (./arch/x86/include/asm/irqflags.h:40 ./arch/x86/include/asm/irqflags.h:75 arch/x86/mm/fault.c:1470 arch/x86/mm/fault.c:1518) ? asm_exc_page_fault (./arch/x86/include/asm/idtentry.h:570) ? iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat xt_find_table_lock (net/netfilter/x_tables.c:1259) xt_request_find_table_lock (net/netfilter/x_tables.c:1287) get_info (net/ipv4/netfilter/ip_tables.c:965)		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? security_capable (security/security.c:809 (discriminator 13)) ? ns_capable (kernel/capability.c:376 kernel/capability.c:397) ? do_ipt_get_ctl (net/ipv4/netfilter/ip_tables.c:1656) ? bpfilter_send_req (net/bpfilter/bpfilter_kern.c:52) bpfilter nf_getsockopt (net/netfilter/nf_sockopt.c:116) ip_getsockopt (net/ipv4/ip_sockglue.c:1827) __sys_getsockopt (net/socket.c:2327) __x64_sys_getsockopt (net/socket.c:2342 net/socket.c:2339 net/socket.c:2339) do_syscall_64 (arch/x86/entry/common.c:51 arch/x86/entry/common.c:81) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121)		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0033:0x7f62844685ee Code: 48 8b 0d 45 28 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 37 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 0a c3 66 0f 1f 84 00 00 00 00 00 48 8b 15 09 RSP: 002b:00007ffd1f83d638 EFLAGS: 00000246 ORIG_RAX: 0000000000000037 RAX: ffffffffffffffda RBX: 00007ffd1f83d680 RCX: 00007f62844685ee RDX: 0000000000000040 RSI: 0000000000000000 RDI: 0000000000000004 RBP: 0000000000000004 R08: 00007ffd1f83d670 R09: 0000558798ffa2a0 R10: 00007ffd1f83d680 R11:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000246 R12: 00007ffd1f83e3b2 R13: 00007f6284 ---truncated--- **CVE ID: CVE-2024-42270**		
Affected Version(s): From (including) 5.15.15 Up to (excluding) 5.15.37					
Out-of-bounds Read	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix crash due to out of bounds access into reg2btf_ids. When commit e6ac2450d6de ("bpf: Support bpf program calling kernel function") added kfunc support, it defined reg2btf_ids as a cheap way to translate the verifier reg type to the appropriate btf_vmlinux BTF ID, however commit c25b2ae13603 ("bpf: Replace PTR_TO_XXX_OR_NULL with PTR_TO_XXX |	https://git.kernel.org/stable/c/45ce4b4f9009102cd9f581196d480a59208690c1, https://git.kernel.org/stable/c/8c39925e98d498b9531343066ef82ae39e41adae, https://git.kernel.org/stable/c/f0ce1bc9e0235dd7412240be493d7ea65ed9eadc	O-LIN-LINU-030924/1234

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PTR_MAYBE_NULL ") moved the __BPF_REG_TYPE_MAX from the last member of bpf_reg_type enum to after the base register types, and defined other variants using type flag composition. However, now, the direct usage of reg->type to index into reg2btf_ids may no longer fall into __BPF_REG_TYPE_MAX range, and hence lead to out of bounds access and kernel crash on dereference of bad pointer. **CVE ID: CVE-2022-48929**		
Affected Version(s): From (including) 5.16 Up to (excluding) 5.16.12					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/cma: Do not change route.addr.src_addr outside state checks	https://git.kernel.org/stable/c/00265efbd3e5705038c9492a434fda8cf960c8a2, https://git.kernel.org/stable/c/22e9f71072fa605cbf033158db58e0790101928d,	O-LIN-LINU-030924/1235

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If the state is not idle then resolve_prepare_src() should immediately fail and no change to global state should happen. However, it unconditionally overwrites the src_addr trying to build a temporary any address. For instance if the state is already RDMA_CM_LISTEN then this will corrupt the src_addr and would cause the test in cma_cancel_operation(): if (cma_any_addr(cma_src_addr(id_priv)) && !id_priv->cma_dev) Which would manifest as this trace from syzkaller: BUG: KASAN: use-after-free in	https://git.kernel.org/stable/c/5b1cef5798b4fd6e4fd5522e7b8a26248beeacaa	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__list_add_valid+0x93/0xa0 lib/list_debug.c:26 Read of size 8 at addr ffff8881546491e0 by task syz-executor.1/32204 CPU: 1 PID: 32204 Comm: syz-executor.1 Not tainted 5.12.0-rc8-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: __dump_stack lib/dump_stack.c:79 [inline] dump_stack+0x141/0x1d7 lib/dump_stack.c:120 print_address_description.constprop.0.cold+0x5b/0x2f8 mm/kasan/report.c:232 __kasan_report mm/kasan/report.c:399 [inline] kasan_report.cold+		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x7c/0xd8 mm/kasan/report.c:416 __list_add_valid+0x93/0xa0 lib/list_debug.c:26 __list_add include/linux/list.h:67 [inline] list_add_tail include/linux/list.h:100 [inline] cma_listen_on_all drivers/infiniband/core/cma.c:2557 [inline] rdma_listen+0x787/0xe00 drivers/infiniband/core/cma.c:3751 ucma_listen+0x16a/0x210 drivers/infiniband/core/ucma.c:1102 ucma_write+0x259/0x350 drivers/infiniband/core/ucma.c:1732 vfs_write+0x28e/0xa30 fs/read_write.c:603 ksys_write+0x1ee/0x250		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	fs/read_write.c:658 do_syscall_64+0x2d/0x70 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x44/0xae This is indicating that an rdma_id_private was destroyed without doing cma_cancel_listens(). Instead of trying to re-use the src_addr memory to indirectly create an any address derived from the dst build one explicitly on the stack and bind to that as any other normal flow would do. rdma_bind_addr() will copy it over the src_addr once it knows the state is valid. This is similar to commit		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bc0bdc5afaa7 ("RDMA/cma: Do not change route.addr.src_addr.ss_family") **CVE ID: CVE-2022-48925**		
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption.	https://git.kernel.org/stable/c/33222d1571d7ce8c1c75f6b488f38968fa93d2d9, https://git.kernel.org/stable/c/4ce247af3f30078d5b97554f1ae6200a0222c15a, https://git.kernel.org/stable/c/669c2b178956718407af5631ccbc61c24413f038	O-LIN-LINU-030924/1236

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4 [361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1:irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1:irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1:irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1:irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c **CVE ID: CVE-2022-48926**		
Out-of-bounds Write	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: iio: adc: tsc2046: fix memory corruption by preventing array overflow On one side we have indio_dev->num_channels	https://git.kernel.org/stable/c/082d2c047b0d305bb0b6e9f9d671a09470e2db2d, https://git.kernel.org/stable/c/0cb9b2f73c182d242a640e512f4785c7c504512f, https://git.kernel.org/stable/c/b7a78a8adaa8849c02f174d707	O-LIN-LINU-030924/1237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			includes all physical channels + timestamp channel. On other side we have an array allocated only for physical channels. So, fix memory corruption by ARRAY_SIZE() instead of num_channels variable. Note the first case is a cleanup rather than a fix as the software timestamp channel bit in active_scanmask is never set by the IIO core. **CVE ID: CVE-2022-48927**	aead0f85dca0da	
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: make apf token non-zero to fix bug In current async pagefault logic, when a page is ready, KVM relies on	https://git.kernel.org/stable/c/4c3644b6c96c5daa5149e5abddc07234eea47c7c, https://git.kernel.org/stable/c/62040f5cd7d937de547836e747b6aa8212fec573, https://git.kernel.org/stable/c/6f3c1fc53d86d580d8d6d749c	O-LIN-LINU-030924/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kvm_arch_can_dequeue_async_page_present() to determine whether to deliver a READY event to the Guest. This function test token value of struct kvm_vcpu_pv_apf_data, which must be reset to zero by Guest kernel when a READY event is finished by Guest. If value is zero meaning that a READY event is done, so the KVM can deliver another. But the kvm_arch_setup_async_pf() may produce a valid token with zero value, which is confused with previous mention and may lead the loss of this READY event. This bug may cause task blocked forever in Guest: INFO: task stress:7532	4af23705e4f6f79	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	blocked for more than 1254 seconds. Not tainted 5.10.0 #16 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:stress state:D stack: 0 pid: 7532 ppid: 1409 flags:0x00000080 Call Trace: __schedule+0x1e7/0x650 schedule+0x46/0xb0 kvm_async_pf_task_wait_schedule+0xad/0xe0 ? exit_to_user_mode_prepare+0x60/0x70 __kvm_handle_async_pf+0x4f/0xb0 ? asm_exc_page_fault+0x8/0x30 exc_page_fault+0x6f/0x110		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? asm_exc_page_fault+0x8/0x30 asm_exc_page_fault+0x1e/0x30 RIP: 0033:0x402d00 RSP: 002b:00007ffd31912500 EFLAGS: 00010206 RAX: 0000000000071000 RBX: ffffffffffffffff RCX: 00000000021a32b0 RDX: 000000000007d011 RSI: 000000000007d000 RDI: 00000000021262b0 RBP: 00000000021262b0 R08: 0000000000000003 R09: 0000000000000086 R10: 00000000000000eb R11: 00007fefbdf2baa0 R12: 0000000000000000 R13: 000000000000000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2 R14: 000000000007d000 R15: 0000000000001000 **CVE ID: CVE-2022-48943**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: fix memory leak in int3400_notify() It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies 4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65 NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b	https://git.kernel.org/stable/c/2e798814e01827871938ff172d2b2ccf1e74b355, https://git.kernel.org/stable/c/33c73a4d7e7b19313a6b417152f5365016926418, https://git.kernel.org/stable/c/3abea10e6a8f0e7804ed4c124bea2d15aca977c8	O-LIN-LINU-030924/1239

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6b 6b 6b a5 rmal.kkkkkkkkkk. backtrace: [<ffffffff9c502c3e>] __kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0 [<ffffffff9c7b7d6e>] kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>] acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0 [<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff9c2cb4dd>] kthread+0xfd/0x130 [<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly. **CVE ID: CVE-2022-48924**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function. **CVE ID: CVE-2022-48928**	https://git.kernel.org/stable/c/0f88722313645a903f4d420ba61ddc690ec2481d, https://git.kernel.org/stable/c/1aa12ecfdcbafebc218910ec47acf6262e600cf5, https://git.kernel.org/stable/c/53d43a9c8dd224e66559fe86af1e473802c7130e	O-LIN-LINU-030924/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync() **CVE ID: CVE-2022-48930**	https://git.kernel.org/stable/c/081bdc9fe05bb23248f5effb6f811da3da4b8252, https://git.kernel.org/stable/c/4752fafb461821f8c8581090c923ababba68c5bd, https://git.kernel.org/stable/c/8cc342508f9e7fdccd2e9758ae9d52aff72dab7f	O-LIN-LINU-030924/1241
Out-of-bounds Read	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: DR, Fix slab-out-of-bounds in mlx5_cmd_dr_create_fte When adding a rule with 32 destinations, we hit the following out-of-band access issue:	https://git.kernel.org/stable/c/0aec12d97b2036af0946e3d582144739860ac07b, https://git.kernel.org/stable/c/4ad319cdfbe555b4ff67bc608736c46a6930c848	O-LIN-LINU-030924/1242

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KASAN: slab-out-of-bounds in mlx5_cmd_dr_create_fte+0x18ee/0x1e70 This patch fixes the issue by both increasing the allocated buffers to accommodate for the needed actions and by checking the number of actions to prevent this issue when a rule with too many actions is provided. **CVE ID: CVE-2022-48932**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix memory leak during stateful obj update stateful objects can be updated from the control plane. The transaction logic allocates a temporary object for this purpose. The ->init function was called for this	https://git.kernel.org/stable/c/34bb90e407e3288f610558beaae54ecaa32b11c4, https://git.kernel.org/stable/c/53026346a94c43f35c32b18804041bc483271d87, https://git.kernel.org/stable/c/7e9880e81d3fd6a43c202f205717485290432826	O-LIN-LINU-030924/1243

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object, so plain kfree() leaks resources. We must call ->destroy function of the object. nft_obj_destroy does this, but it also decrements the module refcount, but the update path doesn't increment it. To avoid special-casing the update object release, do module_get for the update case too and release it via nft_obj_destroy(). **CVE ID: CVE-2022-48933**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: flower: Fix a potential leak in nfp_tunnel_add_shared_mac() ida_simple_get() returns an id between min (0) and max	https://git.kernel.org/stable/c/3a14d0888eb4b0045884126acc69abfb7b87814d, https://git.kernel.org/stable/c/4086d2433576baf85f0e538511df97c8101e0a10, https://git.kernel.org/stable/c/5ad5886f85b6bd893e3ed1901	O-LIN-LINU-030924/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NFP_MAX_MAC_INDEX) inclusive. So NFP_MAX_MAC_INDEX (0xff) is a valid id. In order for the error handling path to work correctly, the 'invalid' value for 'ida_idx' should not be in the 0..NFP_MAX_MAC_INDEX range, inclusive. So set it to -1. **CVE ID: CVE-2022-48934**	3765fb0c243c069	
Use After Free	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unregister flowtable hooks on netns exit Unregister flowtable hooks before they are releases via nf_tables_flowtable_destroy() otherwise hook core reports UAF.	https://git.kernel.org/stable/c/6069da443bf65f513bb507bb21e2f87cfb1ad0b6, https://git.kernel.org/stable/c/88c795491bf45a8c08a0f94c9ca4f13722e51013, https://git.kernel.org/stable/c/8ffb8ac3448845f65634889b051bd65e4dee484b	O-LIN-LINU-030924/1245

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: KASAN: use-after-free in nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 Read of size 4 at addr ffff8880736f7438 by task syz-executor579/3666 CPU: 0 PID: 3666 Comm: syz-executor579 Not tainted 5.16.0-rc5-syzkaller #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 lib/dump_stack.c:88 [inline] lib/dump_stack.c:106 dump_stack_lvl+0x1dc/0x2d8 lib/dump_stack.c:1		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			06 lib/dump_stack.c:106 print_address_description+0x65/0x380 mm/kasan/report.c:247 mm/kasan/report.c:247 __kasan_report mm/kasan/report.c:433 [inline] __kasan_report mm/kasan/report.c:433 [inline] mm/kasan/report.c:450 kasan_report+0x19a/0x1f0 mm/kasan/report.c:450 mm/kasan/report.c:450 nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 __nf_register_net_hook+0x27e/0x8d0 net/netfilter/core.c:429 net/netfilter/core.c:429 nf_register_net_hoo		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k+0xaa/0x180 net/netfilter/core.c:571 net/netfilter/core.c:571 nft_register_flowtable_net_hooks+0x3c5/0x730 net/netfilter/nf_tables_api.c:7232 net/netfilter/nf_tables_api.c:7232 nf_tables_newflowtable+0x2022/0x2cf0 net/netfilter/nf_tables_api.c:7430 net/netfilter/nf_tables_api.c:7430 nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/nfnetlink.c:652 nfnetlink_rcv+0x10e6/0x2550 net/netfilter/nfnetlink.c:652 net/netfilter/nfnetlink.c:652 __nft_release_hook() calls nft_unregister_flowtable_net_hooks() which only unregisters the hooks, then after RCU grace period, it is guaranteed that no packets add new entries to the flowtable (no flow offload rules and flowtable hooks are reachable from packet path), so it is safe to call nf_flow_table_free() which cleans up the remaining entries from the flowtable (both software and hardware) and it unbinds the flow_block. **CVE ID: CVE-2022-48935**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: CDC-NCM: avoid overflow in sanity checking A broken device may give an extreme offset like 0xFFF0 and a reasonable length for a fragment. In the sanity check as formulated now, this will create an integer overflow, defeating the sanity check. Both offset and offset + len need to be checked in such a manner that no overflow can occur. And those quantities should be unsigned. **CVE ID: CVE-2022-48938**	https://git.kernel.org/stable/c/49909c9f8458cacb5b241106cba65aba5a6d8f4c, https://git.kernel.org/stable/c/69560efa001397ebb8dc1c3e6a3ce00302bb9f7f, https://git.kernel.org/stable/c/7b737e47b87589031f0d4657f6d7b0b770474925	O-LIN-LINU-030924/1246
Improper Restriction of Operations within the Bounds of a	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/719d1c2524c89ada78c4c9202641c1d9e942a322,	O-LIN-LINU-030924/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			bpf: Fix crash due to incorrect copy_map_value When both bpf_spin_lock and bpf_timer are present in a BPF map value, copy_map_value needs to skirt both objects when copying a value into and out of the map. However, the current code does not set both s_off and t_off in copy_map_value, which leads to a crash when e.g. bpf_spin_lock is placed in map value with bpf_timer, as bpf_map_update_elem call will be able to overwrite the other timer object. When the issue is not fixed, an overwriting can produce the following splat:	https://git.kernel.org/stable/c/a8abb0c3dc1e28454851a00f8b7333d9695d566c, https://git.kernel.org/stable/c/eca9bd215d2233de79d930fa97aefbce03247a98	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[root@(none) bpf]# ./test_progs -t timer_crash [15.930339] bpf_testmod: loading out-of-tree module taints kernel. [16.037849] == [16.038458] BUG: KASAN: user-memory-access in __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.038944] Write of size 8 at addr 0000000000043ec0 by task test_progs/325 [16.039399] [16.039514] CPU: 0 PID: 325 Comm: test_progs Tainted: G OE 5.16.0+ #278 [16.039983] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ArchLinux 1.15.0-1 04/01/2014 [16.040485] Call Trace:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16.040645] <TASK> [16.040805] dump_stack_lvl+0x59/0x73 [16.041069] ? __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.041427] kasan_report.cold+0x116/0x11b [16.041673] ? __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042040] __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042328] ? memcpy+0x39/0x60 [16.042552] ? pv_hash+0xd0/0xd0 [16.042785] ? lockdep_hardirqs_off+0x95/0xd0 [16.043079] __bpf_spin_lock_irqsave+0xdf/0xf0 [16.043366] ? bpf_get_current_comm+0x50/0x50 [16.043608] ? jhash+0x11a/0x270		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16.043848] bpf_timer_cancel+0x34/0xe0 [16.044119] bpf_prog_c4ea1c0f7449940d_sys_enter+0x7c/0x81 [16.044500] bpf_trampoline_6442477838_0+0x36/0x1000 [16.044836] __x64_sys_nanosleep+0x5/0x140 [16.045119] do_syscall_64+0x59/0x80 [16.045377] ? lock_is_held_type+0xe4/0x140 [16.045670] ? irqentry_exit_to_user_mode+0xa/0x40 [16.046001] ? mark_held_locks+0x24/0x90 [16.046287] ? asm_exc_page_fault+0x1e/0x30 [16.046569] ? asm_exc_page_fault+0x8/0x30 [16.046851] ? lockdep_hardirqs_on+0x7e/0x100 [16.047137] entry_SYSCALL_64_after_hwframe+0x44/0xae		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16.047405] RIP: 0033:0x7f9e4831718d [16.047602] Code: b4 0c 00 0f 05 eb a9 66 0f 1f 44 00 00 f3 0f 1e fa 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 8b 0d b3 6c 0c 00 f7 d8 64 89 01 48 [16.048764] RSP: 002b:00007fff488086b8 EFLAGS: 00000206 ORIG_RAX: 0000000000000023 [16.049275] RAX: ffffffffffffffda RBX: 00007f9e48683740 RCX: 00007f9e4831718d [16.049747] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 00007fff488086d0 [16.050225] RBP: 00007fff488086f0 R08: 00007fff488085d7 R09: 00007f9e4cb594a0 [16.050648] R10: 000000000000000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 R11: 0000000000000206 R12: 00007f9e484cde30 [16.051124] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [16.051608] </TASK> [16.051762] == **CVE ID: CVE-2022-48940**		
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: hwmon: Handle failure to register sensor with thermal zone correctly If an attempt is made to a sensor with a thermal zone and it fails, the call to devm_thermal_zone_of_sensor_registe	https://git.kernel.org/stable/c/1b5f517cca36292076d9e38fa6e33a257703e62e, https://git.kernel.org/stable/c/7efe8499cb90651c540753f4269d2d43ede14223, https://git.kernel.org/stable/c/8a1969e14ad93663f9a3ed02ccc2138da9956a0e	O-LIN-LINU-030924/1248

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			r() may return -ENODEV. This may result in crashes similar to the following. Unable to handle kernel NULL pointer dereference at virtual address 00000000000003cd ... Internal error: Oops: 96000021 [#1] PREEMPT SMP ... pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : mutex_lock+0x18/0x60 lr : thermal_zone_device_update+0x40/0x2e0 sp : ffff800014c4fc60 x29: ffff800014c4fc60 x28: ffff365ee3f6e000 x27: ffffdde218426790 x26: ffff365ee3f6e000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x25: 0000000000000000 x24: ffff365ee3f6e000 x23: ffffdde218426870 x22: ffff365ee3f6e000 x21: 00000000000003cd x20: ffff365ee8bf3308 x19: ffffffffffffffed x18: 0000000000000000 x17: ffffdde21842689c x16: ffffdde1cb7a0b7c x15: 0000000000000040 x14: ffffdde21a4889a0 x13: 0000000000000228 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000000001120000 x7 : 000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1 x6 : 0000000000000000 x5 : 0068000878e20f07 x4 : 0000000000000000 x3 : 00000000000003cd x2 : ffff365ee3f6e000 x1 : 0000000000000000 x0 : 00000000000003cd Call trace: mutex_lock+0x18/0x60 hwmon_notify_event+0xfc/0x110 0xffffdde1cb7a0a90 0xffffdde1cb7a0b7c irq_thread_fn+0x2c/0xa0 irq_thread+0x134/0x240 kthread+0x178/0x190		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ret_from_fork+0x10/0x20 Code: d503201f d503201f d2800001 aa0103e4 (c8e47c02) Jon Hunter reports that the exact call sequence is: hwmon_notify_event() --> hwmon_thermal_notify() --> thermal_zone_device_update() --> update_temperature() --> mutex_lock() The hwmon core needs to handle all errors returned from calls to devm_thermal_zone_of_sensor_register(). If the call fails with -ENODEV, report that the sensor was not attached to a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thermal zone but continue to register the hwmon device. **CVE ID: CVE-2022-48942**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is: A --> B --> C --> D A <-- B <-- C <-- D delete list_head *B | delete list_head *C	https://git.kernel.org/stable/c/3aadfd46858b1f64d4d6a0654b863e21aabff975, https://git.kernel.org/stable/c/40805099af11f68c5ca7dbcfacf455da8f99f622, https://git.kernel.org/stable/c/84ec758fb2daa236026506868c8796b0500c047d	O-LIN-LINU-030924/1249

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

* stands for all versions

<table>
<tr><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description &amp; CVE ID</th><th>Patch</th><th>NCIIPC ID</th></tr>
<tr><td></td><td></td><td></td><td>--------------------------------|----------------------------------
configfs_unregister_subsystem | configfs_unregister_subsystem
unlink_group | unlink_group
unlink_obj | unlink_obj
list_del_init | list_del_init
__list_del_entry | __list_del_entry
__list_del | __list_del
// next == C |
next->prev = prev |
| next->prev = prev
prev->next = next |
| // prev == B
| prev->next = next

Fix this by adding mutex when calling link_group() or unlink_group(),
but parent configfs_subsystem is NULL when config_item is root.</td><td></td><td></td></tr>
</table>

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			So I create a mutex configfs_subsystem _mutex. **CVE ID: CVE-2022-48931**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: ice: fix concurrent reset and removal of VFs Commit c503e63200c6 ("ice: Stop processing VF messages during teardown") introduced a driver state flag, ICE_VF_DEINIT_IN_PROGRESS, which is intended to prevent some issues with concurrently handling messages from VFs while tearing down the VFs. This change was motivated by crashes caused while tearing down and bringing up VFs in rapid succession.	https://git.kernel.org/stable/c/05ae1f0fe9c6c5ead08b306e665763a352d20716, https://git.kernel.org/stable/c/2a3e61de89bab6696aa28b70030eb119968c5586, https://git.kernel.org/stable/c/3c805fce07c9dbc47d8a9129c7c5458025951957	O-LIN-LINU-030924/1250

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It turns out that the fix actually introduces issues with the VF driver caused because the PF no longer responds to any messages sent by the VF during its .remove routine. This results in the VF potentially removing its DMA memory before the PF has shut down the device queues. Additionally, the fix doesn't actually resolve concurrency issues within the ice driver. It is possible for a VF to initiate a reset just prior to the ice driver removing VFs. This can result in the remove task concurrently operating while the VF is being reset. This results in similar memory corruption and panics purportedly		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed by that commit. Fix this concurrency at its root by protecting both the reset and removal flows using the existing VF cfg_lock. This ensures that we cannot remove the VF while any outstanding critical tasks such as a virtchnl message or a reset are occurring. This locking change also fixes the root cause originally fixed by commit c503e63200c6 ("ice: Stop processing VF messages during teardown"), so we can simply revert it. Note that I kept these two changes together because simply reverting the original commit alone would leave the driver vulnerable to worse race		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions. **CVE ID: CVE-2022-48941**		
Improper Locking	22-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: io_uring: add a schedule point in io_add_buffers() Looping ~65535 times doing kmalloc() calls can trigger soft lockups, especially with DEBUG features (like KASAN). [253.536212] watchdog: BUG: soft lockup - CPU#64 stuck for 26s! [b219417889:12575] [253.544433] Modules linked in: vfat fat i2c_mux_pca954x i2c_mux spidev cdc_acm xhci_pci xhci_hcd sha3_generic gq(O) [253.544451] CPU: 64 PID: 12575 Comm: b219417889 Tainted: G S O	https://git.kernel.org/stable/c/4a93c6594613c3429b6f30136fff115c7f803af4, https://git.kernel.org/stable/c/8f3cc3c5bc43d03b5748ac4fb8d180084952c36a, https://git.kernel.org/stable/c/c718ea4e7382e18957ed0e88a5f855e2122d9c00	O-LIN-LINU-030924/1251

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.17.0-smp-DEV #801 [253.544457] RIP: 0010:kernel_text_address (./include/asm-generic/sections.h:192 ./include/linux/kallsyms.h:29 kernel/extable.c:67 kernel/extable.c:98) [253.544464] Code: 0f 93 c0 48 c7 c1 e0 63 d7 a4 48 39 cb 0f 92 c1 20 c1 0f b6 c1 5b 5d c3 90 0f 1f 44 00 00 55 48 89 e5 41 57 41 56 53 48 89 fb <48> c7 c0 00 00 80 a0 41 be 01 00 00 00 48 39 c7 72 0c 48 c7 c0 40 [253.544468] RSP: 0018:ffff8882d8baf4c0 EFLAGS: 00000246 [253.544471] RAX: 1ffff1105b175e00 RBX: ffffffffa13ef09a RCX: 00000000a13ef001 [253.544474] RDX: ffffffffa13ef09a RSI: ffff8882d8baf558		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDI: ffffffffa13ef09a [253.544476] RBP: ffff8882d8baf4d8 R08: ffff8882d8baf5e0 R09: 0000000000000004 [253.544479] R10: ffff8882d8baf5e8 R11: ffffffffa0d59a50 R12: ffff8882eab20380 [253.544481] R13: ffffffffa0d59a50 R14: dffffc0000000000 R15: 1ffff1105b175eb0 [253.544483] FS: 00000000016d3380(0000) GS:ffff88af48c00000(0000) knlGS:0000000000000000 [253.544486] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [253.544488] CR2: 00000000004af0f0 CR3: 00000002eabfa004 CR4: 00000000003706e0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[253.544491] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [253.544492] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [253.544494] Call Trace: [253.544496] <TASK> [253.544498] ? io_queue_sqe (fs/io_uring.c:7143) [253.544505] __kernel_text_address (kernel/extable.c:78) [253.544508] unwind_get_return_address (arch/x86/kernel/unwind_frame.c:19) [253.544514] arch_stack_walk (arch/x86/kernel/stacktrace.c:27) [253.544517] ? io_queue_sqe		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(fs/io_uring.c:7143) [253.544521] stack_trace_save (kernel/stacktrace.c:123) [253.544527] ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544531] ? ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544533] ? __kasan_kmalloc (mm/kasan/common.c:524) [253.544535] ? kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544541] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[253.544544] ? __io_queue_sqe (fs/io_uring.c:?) [253.544551] __kasan_kmalloc (mm/kasan/common.c:524) [253.544553] kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544556] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544560] io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544564] ? __kasan_slab_alloc (mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544567] ? __kasan_slab_alloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469)		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[253.544569] ? kmem_cache_alloc_bulk (mm/slab.h:732 mm/slab.c:3546) [253.544573] ? __io_alloc_req_refill (fs/io_uring.c:2078) [253.544578] ? io_submit_sqes (fs/io_uring.c:7441) [253.544581] ? __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uring.c:10096) [253.544584] ? __x64_sys_io_uring_enter (fs/io_uring.c:10096) [253.544587] ? do_syscall_64 (arch/x86/entry/common.c:50 arch/x86/entry/common.c:80) [253.544590] ? entry_SYSCALL_64_after_hwframe (??:?) [253.544596] __io_queue_sqe (fs/io_uring.c:?) [253.544600] io_queue_sqe		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(fs/io_uring.c:7143) [253.544603] io_submit_sqe (fs/io_uring.c:?) [253.544608] io_submit_sqes (fs/io_uring.c:?) [253.544612] __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uri ---truncated--- **CVE ID: CVE-2022-48937**		
Excessive Iteration	22-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: bpf: Add schedule points in batch ops syzbot reported various soft lockups caused by bpf batch operations. INFO: task kworker/1:1:27 blocked for more than 140 seconds. INFO: task hung in rcu_barrier Nothing prevents batch ops to	https://git.kernel.org/stable/c/75134f16e7dd0007aa474b281935c5f42e79f2c8, https://git.kernel.org/stable/c/7e8099967d0e3ff9d1ae043e80b27fbe46c08417, https://git.kernel.org/stable/c/7ef94bfb08fb9e73defafbd5ddef6b5a0e2ee12b	O-LIN-LINU-030924/1252

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process huge amount of data, we need to add schedule points in them. Note that maybe_wait_bpf_programs(map) calls from generic_map_delete_batch() can be factorized by moving the call after the loop. This will be done later in -next tree once we get this fix merged, unless there is strong opinion doing this optimization sooner. **CVE ID: CVE-2022-48939**		
Affected Version(s): From (including) 5.16 Up to (excluding) 5.16.13					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: fix use-after-free in __nf_register_net_hook()	https://git.kernel.org/stable/c/05f7927b25d2635e87267ff6c79db79fb46cf313, https://git.kernel.org/stable/c/49c24579cec41e32f13d57b337fd28fb208d4a5	O-LIN-LINU-030924/1253

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430 CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #0 Hardware name: Google Google	b, https://git.kernel.org/stable/c/56763f12b0f02706576a088e85ef856deacc98a0	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	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+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218 synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0 net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline] find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101 ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084 __sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsocko		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pt+0xba/0x150 net/socket.c:2188 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: 0033:0x7f65a1ace7d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 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 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12: 00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000 </TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993 prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x35a/0x4a0 mm/slub. ---truncated--- **CVE ID: CVE-2022-48912**		
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: blktrace: fix use after free for struct blk_trace When tracing the whole disk, 'dropped' and 'msg' will be created under 'q->debugfs_dir' and 'bt->dir' is NULL,	https://git.kernel.org/stable/c/30939293262eb433c960c4532a0d59c4073b2b84, https://git.kernel.org/stable/c/6418634238ade86f2b08192928787f39d8afb58c, https://git.kernel.org/stable/c/78acc7dbd84a8c173a0858475	O-LIN-LINU-030924/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thus blk_trace_free() won't remove those files. What's worse, the following UAF can be triggered because of accessing stale 'dropped' and 'msg': == BUG: KASAN: use-after-free in blk_dropped_read+0x89/0x100 Read of size 4 at addr ffff88816912f3d8 by task blktrace/1188 CPU: 27 PID: 1188 Comm: blktrace Not tainted 5.17.0-rc4-next-20220217+ #469 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ?-20190727_073836-4 Call Trace: <TASK>	0845c31611160f2	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dump_stack_lvl+0x34/0x44 print_address_description.constprop.0.cold+0xab/0x381 ? blk_dropped_read+0x89/0x100 ? blk_dropped_read+0x89/0x100 kasan_report.cold+0x83/0xdf ? blk_dropped_read+0x89/0x100 kasan_check_range+0x140/0x1b0 blk_dropped_read+0x89/0x100 ? blk_create_buf_file_callback+0x20/0x20 ? kmem_cache_free+0xa1/0x500 ? do_sys_openat2+0x258/0x460 full_proxy_read+0x8f/0xc0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vfs_read+0xc6/0x260 ksys_read+0xb9/0x150 ? vfs_write+0x3d0/0x3d0 ? fpregs_assert_state_consistent+0x55/0x60 ? exit_to_user_mode_prepare+0x39/0x1e0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fbc080d92fd Code: ce 20 00 00 75 10 b8 00 00 00 00 0f 05 48 3d 01 f0 ff ff 73 31 c3 48 83 1 RSP: 002b:00007fbb95ff9cb0 EFLAGS: 00000293 ORIG_RAX: 0000000000000000 RAX: ffffffffffffffda RBX:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00007fbb95ff9dc0 RCX: 00007fbc080d92fd RDX: 0000000000000100 RSI: 00007fbb95ff9cc0 RDI: 0000000000000045 RBP: 0000000000000045 R08: 0000000000406299 R09: 00000000fffffffd R10: 000000000153afa0 R11: 0000000000000293 R12: 00007fbb780008c0 R13: 00007fbb78000938 R14: 0000000000608b30 R15: 00007fbb780029c8 </TASK> Allocated by task 1050: kasan_save_stack+0x1e/0x40 __kasan_kmalloc+0x81/0xa0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	do_blk_trace_setup+0xcb/0x410 __blk_trace_setup+0xac/0x130 blk_trace_ioctl+0xe9/0x1c0 blkdev_ioctl+0xf1/0x390 __x64_sys_ioctl+0xa5/0xe0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae Freed by task 1050: kasan_save_stack+0x1e/0x40 kasan_set_track+0x21/0x30 kasan_set_free_info+0x20/0x30 __kasan_slab_free+0x103/0x180 kfree+0x9a/0x4c0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	__blk_trace_remove+0x53/0x70 blk_trace_ioctl+0x199/0x1c0 blkdev_common_ioctl+0x5e9/0xb30 blkdev_ioctl+0x1a5/0x390 __x64_sys_ioctl+0xa5/0xe0 do_syscall_64+0x35/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae The buggy address belongs to the object at ffff88816912f380 which belongs to the cache kmalloc-96 of size 96 The buggy address is located 88 bytes inside of 96-byte region [ffff88816912f380, ffff88816912f3e0) The buggy address belongs to the page: page:000000009a1b4e7c refcount:1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	mapcount:0 mapping:0000000000000000 index:0x0f flags: 0x17ffffc0000200(slab|node=0|zone=2|lastcpupid=0x1fffff) raw: 0017ffffc0000200 ffffea00044f1100 dead000000000002 ffff88810004c780 raw: 0000000000000000 0000000000200020 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff88816912f280: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f300: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc >ffff88816912f380: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ^		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff88816912f400: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f480: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc == **CVE ID: CVE-2022-48913**		
Double Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in	https://git.kernel.org/stable/c/147a0e71ccf96df9fc8c2ac500829d8e423ef02c, https://git.kernel.org/stable/c/2fe0e281f7ad0a62259649764228227dd6b2561d, https://git.kernel.org/stable/c/3d6cc9898efdfb062efb74dc18cfc700e082f5d5	O-LIN-LINU-030924/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4 [Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ>		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0 [Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0 ... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	kasan_set_free_info +0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free +0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+ 0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635 /0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae **CVE ID: CVE-2022-48919**		
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1c0b51e62a50e9291764d022ed44549e65d6ab9c, https://git.kern	O-LIN-LINU-030924/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thermal: core: Fix TZ_GET_TRIP NULL pointer dereference Do not call get_trip_hyst() from thermal_genl_cmd_tz_get_trip() if the thermal zone does not define one. **CVE ID: CVE-2022-48915**	el.org/stable/c/3dafbf915c05f83469e791949b5590da2aca2afb, https://git.kernel.org/stable/c/4c294285cec3964b3291772ac0642c2bf440bd1b	
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iwlwifi: mvm: check debugfs_dir ptr before use When "debugfs=off" is used on the kernel command line, iwiwifi's mvm module uses an invalid/unchecked debugfs_dir pointer and causes a BUG: BUG: kernel NULL pointer dereference, address:	https://git.kernel.org/stable/c/5a6248c0a22352f09ea041665d3bd3e18f6f872c, https://git.kernel.org/stable/c/7de1ed755e1ace30d97a724bad32452ed86b653b, https://git.kernel.org/stable/c/fe51975ff13831e794e1bcd0039b305dcad3d7ba	O-LIN-LINU-030924/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			000000000000004f #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP CPU: 1 PID: 503 Comm: modprobe Tainted: G W 5.17.0-rc5 #7 Hardware name: Dell Inc. Inspiron 15 5510/076F7Y, BIOS 2.4.1 11/05/2021 RIP: 0010:iwl_mvm_dbgfs_register+0x692/0x700 [iwlmvm] Code: 69 a0 be 80 01 00 00 48 c7 c7 50 73 6a a0 e8 95 cf ee e0 48 8b 83 b0 1e 00 00 48 c7 c2 54 73 6a a0 be 64 00 00 00 48 8d 7d 8c <48> 8b 48 50 e8 15 22 07 e1 48 8b 43 28 48 8d 55 8c 48 c7 c7 5f 73 RSP: 0018:ffffc90000a0ba68 EFLAGS: 00010246 RAX: ffffffffffffffff RBX:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff88817d6e3328 RCX: ffff88817d6e3328 RDX: ffffffffa06a7354 RSI: 0000000000000064 RDI: ffffc90000a0ba6c RBP: ffffc90000a0bae0 R08: ffffffff824e4880 R09: ffffffffa069d620 R10: ffffc90000a0ba00 R11: ffffffffffffffff R12: 0000000000000000 R13: ffffc90000a0bb28 R14: ffff88817d6e3328 R15: ffff88817d6e3320 FS: 00007f64dd92d740(0000) GS:ffff88847f640000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004f CR3: 000000016fc7900		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1 CR4: 0000000000770ee0 PKRU: 55555554 Call Trace: <TASK> ? iwl_mvm_mac_setup_register+0xbdc/0xda0 [iwlmvm] iwl_mvm_start_post_nvm+0x71/0x100 [iwlmvm] iwl_op_mode_mvm_start+0xab8/0xb30 [iwlmvm] _iwl_op_mode_start+0x6f/0xd0 [iwlwifi] iwl_opmode_register+0x6a/0xe0 [iwlwifi] ? 0xffffffffa0231000 iwl_mvm_init+0x35/0x1000 [iwlmvm] ? 0xffffffffa0231000 do_one_initcall+0x5a/0x1b0 ? kmem_cache_alloc+0x1e5/0x2f0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_init_module+0x1e/0x220 do_init_module+0x48/0x220 load_module+0x2602/0x2bc0 ? __kernel_read+0x145/0x2e0 ? kernel_read_file+0x229/0x290 __do_sys_finit_module+0xc5/0x130 ? __do_sys_finit_module+0xc5/0x130 __x64_sys_finit_module+0x13/0x20 do_syscall_64+0x38/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f64dda564dd Code: 5b 41 5c c3 66 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 1b 29 0f 00 f7 d8 64 89 01 48 RSP: 002b:00007ffdba393f88 EFLAGS: 00000246 ORIG_RAX: 0000000000000139 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f64dda564dd RDX: 0000000000000000 RSI: 00005575399e2ab2 RDI: 0000000000000001 RBP: 000055753a91c5e0 R08: 0000000000000000 R09: 0000000000000002 R10: 0000000000000001 R11: 0000000000000246 R12: 00005575399e2ab2 R13: 000055753a91ceb0 R14:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 R15: 000055753a923018 </TASK> Modules linked in: btintel(+) btmtk bluetooth vfat snd_hda_codec_hdmi fat snd_hda_codec_realtek snd_hda_codec_generic iwlmvm(+) snd_sof_pci_intel_tgl mac80211 snd_sof_intel_hda_common soundwire_intel soundwire_generic_allocation soundwire_cadence soundwire_bus snd_sof_intel_hda snd_sof_pci snd_sof snd_sof_xtensa_dsp snd_soc_hdac_hda snd_hda_ext_core snd_soc_acpi_intel_match snd_soc_acpi snd_soc_core btrfs snd_compress snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec raid6_pq iwlwifi snd_hda_core snd_pcm snd_timer snd soundcore cfg80211 intel_ish_ipc(+) thunderbolt rfkill		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intel_ishtp ucsi_acpi wmi i2c_hid_acpi i2c_hid evdev CR2: 000000000000004f ---[end trace 0000000000000000]--- Check the debugfs_dir pointer for an error before using it. [change to make both conditional] **CVE ID: CVE-2022-48918**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.103					
Improper Check for Unusual or Exceptional Conditions	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in	https://git.kernel.org/stable/c/253405541be2f15ffebdeac2f4cf4b7e9144d12f, https://git.kernel.org/stable/c/2abe350db1aa599eeebc6892237d0bce0f1de62a, https://git.kernel.org/stable/c/5eea127675450583680c8170358bcba43227bd69	O-LIN-LINU-030924/1258

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address. **CVE ID: CVE-2024-42284**		

Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:
			RDMA/iwcm: Fix a use-after-free related to destroying CM IDs
			iw_conn_req_handler() associates a new struct rdma_id_private (conn_id) with
			an existing struct iw_cm_id (cm_id) as follows:
			conn_id->cm_id.iw = cm_id;
			cm_id->context = conn_id;
			cm_id->cm_handler = cma_iw_handler;
			rdma_destroy_id() frees both the cm_id and the struct
				https://git.kernel.org/stable/c/557d035fe88d78dd51664f4dc0e1896c04c97cf6, https://git.kernel.org/stable/c/7f25f296fc9bd0435be14e89bf657cd615a23574, https://git.kernel.org/stable/c/94ee7ff99b87435ec63211f632918dc7f44dac79	O-LIN-LINU-030924/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdma_id_private. Make sure that cm_work_handler() does not trigger a use-after-free by only freeing of the struct rdma_id_private after all pending work has finished. **CVE ID: CVE-2024-42285**		
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered during the actual issue: [66.575408s] [pid:5118,cpu4,QT	https://git.kernel.org/stable/c/166a0bddcc27de41fe13f861c8348e8e53e988c8 , https://git.kernel.org/stable/c/47b3dce100778001cd76f7e9188944b5cb27a76d, https://git.kernel.org/stable/c/7789a1d6792af410aa9b39a1eb237ed24fa2170a	O-LIN-LINU-030924/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QThread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9] dump_backtrace+0x0/0x1c0 [66.575469s] [pid:5118,cpu4,QThread,0]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s] [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport] **CVE ID: CVE-2024-42301**		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a DPC event occurs concurrently to	https://git.kernel.org/stable/c/11a1f4bc47362700fcbde717292158873fb847ed, https://git.kernel.org/stable/c/2c111413f38ca5cf87557cab89f6d82b0e3433e7, https://git.kernel.org/stable/c/2cc8973bdc4d6c928ebe38b88090a2cdfe81f42f	O-LIN-LINU-030924/1261

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	hot-removal of the same portion of the hierarchy: The dpc_handler() awaits readiness of the secondary bus below the Downstream Port where the DPC event occurred. To do so, it polls the config space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct pci_dev cause the kernel to oops. That's because pci_bridge_wait_for_secondary_bus() neglects to hold a reference on the child device. Before v6.3, the function was only called on resume from system sleep or on runtime resume. Holding a reference wasn't necessary back then because the pciehp IRQ thread		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the resume_noirq phase. And runtime resume is always awaited before a PCI device is removed.) However starting with v6.3, pci_bridge_wait_for_secondary_bus() is also called on a DPC event. Commit 53b54ad074de ("PCI/DPC: Await readiness of secondary bus after reset"), which introduced that, failed to appreciate that pci_bridge_wait_for_secondary_bus() now needs to hold a reference on the child device because dpc_handler() and pciehp may indeed run concurrently. The commit was		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backported to v5.10+ stable kernels, so that's the oldest one affected. Add the missing reference acquisition. Abridged stack trace: BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464 Comm: irq/53-pcie-dpc 6.9.0 RIP: pci_bus_read_config_dword+0x17/0x50 pci_dev_wait() pci_bridge_wait_for_secondary_bus() dpc_reset_link() pcie_do_recovery() dpc_handler() **CVE ID: CVE-2024-42302**		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/4c9d235630d35db762b85a41	O-LIN-LINU-030924/1262

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: media: venus: fix use after free in vdec_close There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decoding can incur a read after free for inst. Fix it by cancelling the work in vdec_close. **CVE ID: CVE-2024-42313**	49bbb0be9d504c36, https://git.kernel.org/stable/c/66fa52edd32cdbb675f0803b3c4da10ea19b6635, https://git.kernel.org/stable/c/6a96041659e834dc0b172dda4b2df512d63920c2	
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/538a27c8048f081a5ddd286f886eb986fbbc7f80, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			jfs: Fix array-index-out-of-bounds in diFree **CVE ID: CVE-2024-43858**	55b732c8b09b41148eaab2fa8e31b0af47671e00, https://git.kernel.org/stable/c/63f7fdf733add82f126ea00e2e48f6eba15ac4b9	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed when receiving ICMP packets with secmark set while an ICMP raw socket is being created. SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socket before that, causing the null pointer dereference.	https://git.kernel.org/stable/c/0abe35bc48d4ec80424b1f4b3560c0e082cbd5c1, https://git.kernel.org/stable/c/290a6b88e8c19b6636ed1acc733d1458206f7697, https://git.kernel.org/stable/c/347dcb84a4874b5fb375092c08d8cc4069b94f81	O-LIN-LINU-030924/1264

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Drop the packet if label context is not set. BUG: kernel NULL pointer dereference, address: 000000000000004c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1 3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 RIP: 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 89 f0 <8b> 77 4c 39 c6 7e 1f 48 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2 RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 000000000000000e RDX: ffffa92940003be8 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400 R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 R12: ffff8b574c642400 R13: 0000000000000001 R14:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000001 R15: 0000000000000000 FS: 00007fb092ea7640(0000) GS:ffff8b577bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			apparmor_secmark_check+0xec/0x330 security_sock_rcv_skb+0x35/0x50 sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0 ip_local_deliver_finish+0x76/0xa0 __netif_receive_skb_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			56a84f9c97178c57a43a24ec073b45a9d6f01f3a] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 net_rx_action+0x2a4/0x380 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0 common_interrupt+0x86/0xa0 </IRQ> <TASK> asm_common_interrupt+0x26/0x40 RIP: 0010:apparmor_socket_post_create+0xb/0x200 Code: 08 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00 00 48 8b 1d 80 56 3f 02 48 RSP: 0018:ffffa92940ce7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000002 RDI: ffff8b574eaab740 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 0000000000000002 R14: ffff8b574eaab740 R15: ffffffffbd8e4748		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_apparmor_socket_post_create+0x10/0x10 security_socket_post_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys_socket+0x89/0x100 __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc **CVE ID: CVE-2023-52889**		
Use of Uninitialized Resource	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1377de719652d868f5317ba8398b7e74c5f043	O-LIN-LINU-030924/1265

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net: nexthop: Initialize all fields in dumped nexthops struct nexthop_grp contains two reserved fields that are not initialized by nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity): # ip nexthop add id 1 dev lo # ip nexthop add id 101 group 1 # strace -e recvmsg ip nexthop get id 101 ... recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52 The fields are reserved and therefore not	0b, https://git.kernel.org/stable/c/5cc4d71dda2dd4f1520f40e634a527022e48ccd8, https://git.kernel.org/stable/c/6d745cd0e9720282cd291d36b9db528aea18add2	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			currently used. But as they are, they leak kernel memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure. **CVE ID: CVE-2024-42283**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes In psb_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	https://git.kernel.org/stable/c/13b5f3ee94bdbdc4b5f40582aab62977905aedee, https://git.kernel.org/stable/c/2df7aac81070987b0f052985856aa325a38debf6, https://git.kernel.org/stable/c/46d2ef272957879cbe30a884574320e7f7d78692	O-LIN-LINU-030924/1266

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42309		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42310**	https://git.kernel.org/stable/c/08f45102c81ad8bc9f85f7a25e9f64e128edb87d, https://git.kernel.org/stable/c/2d209b2f862f6b8bff549ede541590a8d119da23, https://git.kernel.org/stable/c/977ee4fe895e1729cd36cc26916bbb10084713d6	O-LIN-LINU-030924/1267
Loop with Unreachable Exit Condition ('Infinite Loop')	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ext4: fix infinite loop when replaying fast_commit	https://git.kernel.org/stable/c/0619f7750f2b178a1309808832ab20d85e0ad121, https://git.kernel.org/stable/c/181e63cd595c688194e07332f9944b3a63193d	O-LIN-LINU-030924/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When doing fast_commit replay an infinite loop may occur due to an uninitialized extent_status struct. ext4_ext_determine_insert_hole() does not detect the replay and calls ext4_es_find_extent_range(), which will return immediately without initializing the 'es' variable. Because 'es' contains garbage, an integer overflow may happen causing an infinite loop in this function, easily reproducible using fstest generic/039. This commit fixes this issue by unconditionally initializing the structure in function ext4_es_find_extent_range(). Thanks to Zhang Yi, for figuring out the real problem!	e2, https://git.kernel.org/stable/c/5ed0496e383cb6de120e56991385dce70bbb87c1	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43828		
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: initialize integrity buffer to zero before writing it to media Metadata added by bio_integrity_prep is using plain kmalloc, which leads to random kernel memory being written media. For PI metadata this is limited to the app tag that isn't used by kernel generated metadata, but for non-PI metadata the entire buffer leaks kernel memory. Fix this by adding the __GFP_ZERO flag to allocations for writes. **CVE ID: CVE-2024-43854**	https://git.kernel.org/stable/c/23a19655fb56f241e592041156dfb1c6d04da644, https://git.kernel.org/stable/c/899ee2c3829c5ac14bfc7d3c4a5846c0b709b78f, https://git.kernel.org/stable/c/cf6b45ea7a8df0f61bded1dc4a8561ac6ad143d2	O-LIN-LINU-030924/1269
Allocation of Resources	17-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/1fe97f68fce1ba	O-LIN-LINU-030924/1270

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling		🟨	vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse, then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list. If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong	24bf823bfb0eb0956003473130, https://git.kernel.org/stable/c/22094f5f52e7bc16c5bf9613365049383650b02e, https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03 **CVE ID: CVE-2024-43856**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node value is NULL In imx_rproc_addr_init() "nph = of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So	https://git.kernel.org/stable/c/2fa26ca8b786888673689ccc9da6094150939982, https://git.kernel.org/stable/c/4e13b7c23988c0a13fdca92e94296a3bc2ff9f21, https://git.kernel.org/stable/c/6884fd0283e0831be153fb8d82d9eda8a55acaaa	O-LIN-LINU-030924/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE. [Fixed title to fit within the prescribed 70-75 charcters] **CVE ID: CVE-2024-43860**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.104					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	O-LIN-LINU-030924/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding handling is missing. Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv. **CVE ID: CVE-2024-42271**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.105					
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: wait for previous gc cycles when removing port syzbot hit a use-after-free[1] which is caused because the bridge doesn't make sure that all previous garbage has been collected when removing a port. What happens is: CPU 1 CPU 2 start gc cycle remove port acquire gc lock first wait for lock	https://git.kernel.org/stable/c/0d8b26e10e680c01522d7cc14abe04c3265a928f, https://git.kernel.org/stable/c/1e16828020c674b3be85f52685e8b80f9008f50f, https://git.kernel.org/stable/c/92c4ee25208d0f35dafc3213cdf355fbe449e078	O-LIN-LINU-030924/1273

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			call br_multicasg_gc() directly acquire lock now but free port the port can be freed while grp timers still running Make sure all previous gc cycles have finished by using flush_work before freeing the port. [1] BUG: KASAN: slab-use-after-free in br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 Read of size 8 at addr ffff888071d6d000 by task syz.5.1232/9699 CPU: 1 PID: 9699 Comm: syz.5.1232 Not tainted 6.10.0-rc5-syzkaller-00021-g24ca36a562d6 #0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 call_timer_fn+0x1a3/0x610		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel/time/timer.c:1792 expire_timers kernel/time/timer.c:1843 [inline] __run_timers+0x74b/0xaf0 kernel/time/timer.c:2417 __run_timer_base kernel/time/timer.c:2428 [inline] __run_timer_base kernel/time/timer.c:2421 [inline] run_timer_base+0x111/0x190 kernel/time/timer.c:2437 **CVE ID: CVE-2024-44934**		
Divide By Zero	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time.	https://git.kernel.org/stable/c/6d45e1c948a8b7ed6ceddb14319af69424db730c, https://git.kernel.org/stable/c/8f5ffd2af7274853ff91d6cd62541191d9fbd10d, https://git.kernel.org/stable/c/924f788c906dccaca30acab86c7124371e1d6f2c	O-LIN-LINU-030924/1274

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1 [10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021 [10.017908] Workqueue: events_unbound padata_mt_helper [10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 : [10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30 [10.018147] </TASK> Looking at the padata_mt_helper() function, the only way a divide-by-0 panic can happen is when ps->chunk_size is 0. The way that chunk_size is initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1 no matter what the input parameters are. **CVE ID: CVE-2024-43889**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checker before passing variables Checks null pointer before passing variables to functions. This fixes 3 NULL_RETURNS issues reported by Coverity. **CVE ID: CVE-2024-43902**	https://git.kernel.org/stable/c/1686675405d07f35eae7ff3d13a530034b899df2, https://git.kernel.org/stable/c/4cc2a94d96caeb3c975acdae7351c2f997c32175, https://git.kernel.org/stable/c/8092aa3ab8f7b737a34b71f91492c676a843043a	O-LIN-LINU-030924/1275
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference in apply_state_adjust_rules Check the pointer value to fix	https://git.kernel.org/stable/c/0c065e50445aea2e0a1815f12e97ee49e02cbaac, https://git.kernel.org/stable/c/13937a40aae4efe64592ba48c057ac3c72f7fe82, https://git.kernel.org/stable/c/3a01bf2ca9f860	O-LIN-LINU-030924/1276

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential null pointer dereference **CVE ID: CVE-2024-43907**	fdc88c358567b8fa3033efcf30	
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer dereference to ras_manager Check ras_manager before using it **CVE ID: CVE-2024-43908**	https://git.kernel.org/stable/c/033187a70ba9743c73a810a006816e5553d1e7d4, https://git.kernel.org/stable/c/48cada0ac79e4775236d642e9ec5998a7c7fb7a4, https://git.kernel.org/stable/c/4c11d30c95576937c6c35e6f29884761f2dddb43	O-LIN-LINU-030924/1277
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference for smu7 optimize the code to avoid pass a null pointer (hwmgr->backend) to function smu7_update_edc_leakage_table.	https://git.kernel.org/stable/c/09544cd95c688d3041328a4253bd7514972399bb, https://git.kernel.org/stable/c/1b8aa82b80bd947b68a8ab051d960a0c7935e22d, https://git.kernel.org/stable/c/37b9df457cbcf095963d18f17d6cb7dfa0a03fce	O-LIN-LINU-030924/1278

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43909		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_sock() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be	https://git.kernel.org/stable/c/05e4a0fa248240efd99a539853e844f0f0a9e6a5, https://git.kernel.org/stable/c/1407be30fc17eff918a98e0a990c0e988f11dc84, https://git.kernel.org/stable/c/52319d9d2f522ed939af31af70f8c3a0f0f67e6c	O-LIN-LINU-030924/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and all groups except one would be silently dead.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint(). [0]: Oops: general protection fault,		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89 f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f24e45b96c0(0000) GS:ffff8880b93000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint+0x52a/0x600 net/sctp/input.c:790		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f24e46039b9		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0 R10: 00007f24e45b96c0 R11: 000000000000024		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6 R12: 00007f24e468e42c R13: ---truncated--- **CVE ID: CVE-2024-44935**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.7					
Double Free	21-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: sched/core: Fix use-after-free bug in dup_user_cpus_ptr() Since commit 07ec77a1d4e8 ("sched: Allow task CPU affinity to be restricted on asymmetric systems"), the setting and clearing of user_cpus_ptr are done under pi_lock for arm64 architecture. However, dup_user_cpus_ptr() accesses user_cpus_ptr without any lock protection. Since sched_setaffinity()	https://git.kernel.org/stable/c/7b5cc7fd1789ea5dbb942c9f8207b076d365badc, https://git.kernel.org/stable/c/87ca4f9efbd7cc649ff43b87970888f2812945b8, https://git.kernel.org/stable/c/b22faa21b6230d5eccd233e1b7e0026a5002b287	O-LIN-LINU-030924/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	can be invoked from another process, the process being modified may be undergoing fork() at the same time. When racing with the clearing of user_cpus_ptr in __set_cpus_allowed_ptr_locked(), it can lead to user-after-free and possibly double-free in arm64 kernel. Commit 8f9ea86fdf99 ("sched: Always preserve the user requested cpumask") fixes this problem as user_cpus_ptr, once set, will never be cleared in a task's lifetime. However, this bug was re-introduced in commit 851a723e45d1 ("sched: Always clear user_cpus_ptr in do_set_cpus_allowed()") which allows		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the clearing of user_cpus_ptr in do_set_cpus_allowed(). This time, it will affect all arches. Fix this bug by always clearing the user_cpus_ptr of the newly cloned/forked task before the copying process starts and check the user_cpus_ptr state of the source task under pi_lock. Note to stable, this patch won't be applicable to stable releases. Just copy the new dup_user_cpus_ptr() function over. **CVE ID: CVE-2022-48892**		
NULL Pointer Dereference	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: efi: fix NULL-deref in init error path In cases where runtime services are not supported	https://git.kernel.org/stable/c/4ca71bc0e1995d15486cd7b60845602a28399cb5, https://git.kernel.org/stable/c/585a0b2b3ae7903c6abee3087d09c69e955a7794, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1281

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or have been disabled, the runtime services workqueue will never have been allocated. Do not try to destroy the workqueue unconditionally in the unlikely event that EFI initialisation fails to avoid dereferencing a NULL pointer. **CVE ID: CVE-2022-48879**	5fcf75a8a4c3e7ee9122d143684083c9faf20452	
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.8					
Use After Free	21-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_qca: Fix driver shutdown on closed serdev The driver shutdown callback (which sends EDL_SOC_RESET to the device over serdev) should not be invoked when HCI	https://git.kernel.org/stable/c/272970be3dabd24cbe50e393ffee8f04aec3b9a8, https://git.kernel.org/stable/c/908d1742b6e694e84ead5c62e4b7c1bfbb8b46a3, https://git.kernel.org/stable/c/e84ec6e25df9bb0968599e92eacedaf3a0a5b587	O-LIN-LINU-030924/1282

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	device is not open (e.g. if hci_dev_open_sync() failed), because the serdev and its TTY are not open either. Also skip this step if device is powered off (qca_power_shutdown()). The shutdown callback causes use-after-free during system reboot with Qualcomm Atheros Bluetooth: Unable to handle kernel paging request at virtual address 0072662f67726fd7 ... CPU: 6 PID: 1 Comm: systemd-shutdow Tainted: G W 6.1.0-rt5-00325-g8a5f56bcfcca #8 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tty_driver_flush_buffer+0x4/0x30 serdev_device_write_flush+0x24/0x34 qca_serdev_shutdown+0x80/0x130 [hci_uart] device_shutdown+0x15c/0x260 kernel_restart+0x48/0xac KASAN report: BUG: KASAN: use-after-free in tty_driver_flush_buffer+0x1c/0x50 Read of size 8 at addr ffff16270c2e0018 by task systemd-shutdow/1 CPU: 7 PID: 1 Comm: systemd-shutdow Not tainted 6.1.0-next-20221220-00014-gb85aaf97fb01-dirty #28 Hardware name: Qualcomm		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technologies, Inc. Robotics RB5 (DT) Call trace: dump_backtrace.part.0+0xdc/0xf0 show_stack+0x18/0x30 dump_stack_lvl+0x68/0x84 print_report+0x188/0x488 kasan_report+0xa4/0xf0 __asan_load8+0x80/0xac tty_driver_flush_buffer+0x1c/0x50 ttyport_write_flush+0x34/0x44 serdev_device_write_flush+0x48/0x60 qca_serdev_shutdown+0x124/0x274 device_shutdown+0x1e8/0x350 kernel_restart+0x48/0xb0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__do_sys_reboot+0x244/0x2d0 __arm64_sys_reboot+0x54/0x70 invoke_syscall+0x60/0x190 el0_svc_common.constprop.0+0x7c/0x160 do_el0_svc+0x44/0xf0 el0_svc+0x2c/0x6c el0t_64_sync_handler+0xbc/0x140 el0t_64_sync+0x190/0x194 **CVE ID: CVE-2022-48878**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.6.44					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix extent map use-after-free when adding pages to compressed bio At add_ra_bio_pages()	https://git.kernel.org/stable/c/8e7860543a94784d744c7ce34b78a2e11beefa5c, https://git.kernel.org/stable/c/b7859ff398b6b656e1689daa860eb34837b4bb89, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1283

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			we are accessing the extent map to calculate 'add_size' after we dropped our reference on the extent map, resulting in a use-after-free. Fix this by computing 'add_size' before dropping our extent map reference. **CVE ID: CVE-2024-42314**	c205565e0f2f439f278a4a94ee97b67ef7b56ae8	
Affected Version(s): From (including) 5.16.1 Up to (excluding) 5.16.12					
Out-of-bounds Read	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix crash due to out of bounds access into reg2btf_ids. When commit e6ac2450d6de ("bpf: Support bpf program calling kernel function") added kfunc support, it defined reg2btf_ids as a cheap way to translate the verifier	https://git.kernel.org/stable/c/45ce4b4f9009102cd9f581196d480a59208690c1, https://git.kernel.org/stable/c/8c39925e98d498b9531343066ef82ae39e41adae, https://git.kernel.org/stable/c/f0ce1bc9e0235dd7412240be493d7ea65ed9eadc	O-LIN-LINU-030924/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reg type to the appropriate btf_vmlinux BTF ID, however commit c25b2ae13603 ("bpf: Replace PTR_TO_XXX_OR_NULL with PTR_TO_XXX | PTR_MAYBE_NULL ") moved the __BPF_REG_TYPE_MAX from the last member of bpf_reg_type enum to after the base register types, and defined other variants using type flag composition. However, now, the direct usage of reg->type to index into reg2btf_ids may no longer fall into __BPF_REG_TYPE_MAX range, and hence lead to out of bounds access and kernel crash on dereference of bad pointer. **CVE ID: CVE-2022-48929**		
Affected Version(s): From (including) 5.17 Up to (excluding) 6.6.44					
NULL Pointer	17-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1285

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			vulnerability has been resolved: f2fs: fix to truncate preallocated blocks in f2fs_file_open() chenyuwen reports a f2fs bug as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000011 fscrypt_set_bio_crypt_ctx+0x78/0x1e8 f2fs_grab_read_bio+0x78/0x208 f2fs_submit_page_read+0x44/0x154 f2fs_get_read_data_page+0x288/0x5f4 f2fs_get_lock_data_page+0x60/0x190 truncate_partial_data_page+0x108/0x4fc f2fs_do_truncate_blocks+0x344/0x5f0	298b1e4182d657c3e388adcc29477904e9600ed5, https://git.kernel.org/stable/c/3ba0ae885215b325605ff7ebf6de12ac2adf204d, https://git.kernel.org/stable/c/f44a25a8bfe0c15d33244539696cd9119cf44d18	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f2fs_truncate_blocks+0x6c/0x134 f2fs_truncate+0xd8/0x200 f2fs_iget+0x20c/0x5ac do_garbage_collect+0x5d0/0xf6c f2fs_gc+0x22c/0x6a4 f2fs_disable_checkpoint+0xc8/0x310 f2fs_fill_super+0x14bc/0x1764 mount_bdev+0x1b4/0x21c f2fs_mount+0x20/0x30 legacy_get_tree+0x50/0xbc vfs_get_tree+0x5c/0x1b0 do_new_mount+0x298/0x4cc path_mount+0x33c/0x5fc		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__arm64_sys_mount+0xcc/0x15c invoke_syscall+0x60/0x150 el0_svc_common+0xb8/0xf8 do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 el0t_64_sync_handler+0x88/0xec It is because inode.i_crypt_info is not initialized during below path: - mount - f2fs_fill_super - f2fs_disable_checkpoint - f2fs_gc - f2fs_iget - f2fs_truncate So, let's relocate truncation of preallocated blocks to f2fs_file_open(), after fscrypt_file_open().		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43859		
Affected Version(s): From (including) 5.18 Up to (excluding) 6.1.103					
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix null pointer dereference in resolve_prog_type() for BPF_PROG_TYPE_EXT When loading a EXT program without specifying `attr->attach_prog_fd`, the `prog->aux->dst_prog` will be null. At this time, calling resolve_prog_type() anywhere will result in a null pointer dereference. Example stack trace: [8.107863] Unable to handle kernel NULL pointer dereference at virtual address	https://git.kernel.org/stable/c/9d40fd516aeae6779e3c84c6b96700ca76285847, https://git.kernel.org/stable/c/b29a880bb145e1f1c1df5ab88ed26b1495ff9f09, https://git.kernel.org/stable/c/f7866c35873377313ff94398f17d425b28b71de1	O-LIN-LINU-030924/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000004 [8.108262] Mem abort info: [8.108384] ESR = 0x0000000096000004 [8.108547] EC = 0x25: DABT (current EL), IL = 32 bits [8.108722] SET = 0, FnV = 0 [8.108827] EA = 0, S1PTW = 0 [8.108939] FSC = 0x04: level 0 translation fault [8.109102] Data abort info: [8.109203] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [8.109399] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [8.109614] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [8.109836] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000101354000 [8.110011] [0000000000000004] pgd=00000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00000, p4d=0000000000000000 [8.112624] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [8.112783] Modules linked in: [8.113120] CPU: 0 PID: 99 Comm: may_access_dire Not tainted 6.10.0-rc3-next-20240613-dirty #1 [8.113230] Hardware name: linux,dummy-virt (DT) [8.113390] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [8.113429] pc : may_access_direct_pkt_data+0x24/0xa0 [8.113746] lr : add_subprog_and_kfunc+0x634/0x8e8 [8.113798] sp : ffff80008283b9f0 [8.113813] x29: ffff80008283b9f0 x28: ffff800082795048 x27:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000001 [8.113881] x26: ffff0000c0bb2600 x25: 0000000000000000 x24: 0000000000000000 [8.113897] x23: ffff0000c1134000 x22: 000000000001864f x21: ffff0000c1138000 [8.113912] x20: 0000000000000001 x19: ffff0000c12b8000 x18: ffffffffffffffff [8.113929] x17: 0000000000000000 x16: 0000000000000000 x15: 0720072007200720 [8.113944] x14: 0720072007200720 x13: 0720072007200720 x12: 0720072007200720 [8.113958] x11: 0720072007200720 x10: 0000000000f9fca4 x9 : ffff80008021f4e4 [8.113991] x8 : 010101010101010		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1 x7 : 746f72705f6d656d x6 : 000000001e0e0f5f [8.114006] x5 : 000000000001864f x4 : ffff0000c12b8000 x3 : 000000000000001c [8.114020] x2 : 0000000000000002 x1 : 0000000000000000 x0 : 0000000000000000 [8.114126] Call trace: [8.114159] may_access_direct_pkt_data+0x24/0xa0 [8.114202] bpf_check+0x3bc/0x28c0 [8.114214] bpf_prog_load+0x658/0xa58 [8.114227] __sys_bpf+0xc50/0x2250 [8.114240] __arm64_sys_bpf+0x28/0x40 [8.114254] invoke_syscall.constprop.0+0x54/0xf0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[8.114273] do_el0_svc+0x4c/0xd8 [8.114289] el0_svc+0x3c/0x140 [8.114305] el0t_64_sync_handler+0x134/0x150 [8.114331] el0t_64_sync+0x168/0x170 [8.114477] Code: 7100707f 54000081 f9401c00 f9403800 (b9400403) [8.118672] ---[end trace 0000000000000000]--- One way to fix it is by forcing `attach_prog_fd` non-empty when bpf_prog_load(). But this will lead to `libbpf_probe_bpf_prog_type` API broken which use verifier log to probe prog type and will log nothing if we reject invalid EXT prog before bpf_check().		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Another way is by adding null check in resolve_prog_type(). The issue was introduced by commit 4a9c7bbe2ed4 ("bpf: Resolve to prog->aux->dst_prog->type only for BPF_PROG_TYPE_EXT") which wanted to correct type resolution for BPF_PROG_TYPE_TRACING programs. Before that, the type resolution of BPF_PROG_TYPE_EXT prog actually follows the logic below: prog->aux->dst_prog ? prog->aux->dst_prog->type : prog->type; It implies that when EXT program is not yet attached to `dst_prog`, the prog type should be EXT itself. This code		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			worked fine in the past. So just keep using it. Fix this by returning `prog->type` for BPF_PROG_TYPE_EXT if `dst_prog` is not present in resolve_prog_type(). **CVE ID: CVE-2024-43837**		
Affected Version(s): From (including) 5.18 Up to (excluding) 6.1.7					
N/A	21-Aug-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd: Fix refcount leak in amd_pmc_probe pci_get_domain_bus_and_slot() takes reference, the caller should release the reference by calling pci_dev_put() after use. Call pci_dev_put() in the error path to fix this. **CVE ID: CVE-2022-48881**	https://git.kernel.org/stable/c/3944162821295993ec89992dec98ab6be6306cc0, https://git.kernel.org/stable/c/ccb32e2be14271a60e9ba89c6d5660cc9998773c	O-LIN-LINU-030924/1287
Affected Version(s): From (including) 5.18 Up to (excluding) 6.1.8					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	21-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix use-after-free and race in fastrpc_map_find Currently, there is a race window between the point when the mutex is unlocked in fastrpc_map_lookup and the reference count increasing (fastrpc_map_get) in fastrpc_map_find, which can also lead to use-after-free. So lets merge fastrpc_map_find into fastrpc_map_lookup which allows us to both protect the maps list by also taking the &fl->lock spinlock and the reference count, since the spinlock will be released only after. Add take_ref argument to make	https://git.kernel.org/stable/c/9446fa1683a7e3937d9970248ced427c1983a1c5, https://git.kernel.org/stable/c/a50c5c25b6e7d2824698c0e6385f882a18f4a498	O-LIN-LINU-030924/1288

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this suitable for all callers. **CVE ID: CVE-2022-48874**		
Affected Version(s): From (including) 5.19 Up to (excluding) 6.1.103					
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Fix NULL pointer dereference in adding ancillary links In v4l2_async_create_ancillary_links(), ancillary links are created for lens and flash sub-devices. These are sub-device to sub-device links and if the async notifier is related to a V4L2 device, the source sub-device of the ancillary link is NULL, leading to a NULL pointer dereference. Check the notifier's sd field is non-NULL in v4l2_async_create_ancillary_links().	https://git.kernel.org/stable/c/249212ceb4187783af3801c57b92a5a25d410621, https://git.kernel.org/stable/c/9b4667ea67854f0b116fe22ad11ef5628c5b5b5f, https://git.kernel.org/stable/c/b87e28050d9b0959de24574d587825cfab2f13fb	O-LIN-LINU-030924/1289

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Sakari Ailus: Reword the subject and commit messages slightly.] **CVE ID: CVE-2024-43833**		
Affected Version(s): From (including) 5.19 Up to (excluding) 6.1.7					
Missing Release of Memory after Effective Lifetime	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: Fix memory leak in msm_mdss_parse_data_bus_icc_path of_icc_get() alloc resources for path1, we should release it when not need anymore. Early return when IS_ERR_OR_NULL(path0) may leak path1. Defer getting path1 to fix this. Patchwork: https://patchwork.freedesktop.org/patch/514264/ **CVE ID: CVE-2022-48888**	https://git.kernel.org/stable/c/45dac1352b55b1d8cb17f218936b2bc2bc1fb4ee, https://git.kernel.org/stable/c/c6fa1de83fd87267ab24359e6fa52f98f5cee3f9	O-LIN-LINU-030924/1290
Affected Version(s): From (including) 5.3 Up to (excluding) 5.4.282					
Use of Uninitialized Resource	17-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/1377de719652	O-LIN-LINU-030924/1291

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: net: nexthop: Initialize all fields in dumped nexthops struct nexthop_grp contains two reserved fields that are not initialized by nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity): # ip nexthop add id 1 dev lo # ip nexthop add id 101 group 1 # strace -e recvmsg ip nexthop get id 101 ... recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52	d868f5317ba8398b7e74c5f0430b, https://git.kernel.org/stable/c/5cc4d71dda2dd4f1520f40e634a527022e48ccd8, https://git.kernel.org/stable/c/6d745cd0e9720282cd291d36b9db528aea18add2	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The fields are reserved and therefore not currently used. But as they are, they leak kernel memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure. **CVE ID: CVE-2024-42283**		
Affected Version(s): From (including) 5.4 Up to (excluding) 5.4.182					
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix memory leak during stateful obj update stateful objects can be updated from the control plane. The transaction logic allocates a temporary object for this purpose. The ->init function was called for this object, so plain kfree() leaks	https://git.kernel.org/stable/c/34bb90e407e3288f610558beaae54ecaa32b11c4, https://git.kernel.org/stable/c/53026346a94c43f35c32b18804041bc483271d87, https://git.kernel.org/stable/c/7e9880e81d3fd6a43c202f205717485290432826	O-LIN-LINU-030924/1292

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources. We must call ->destroy function of the object. nft_obj_destroy does this, but it also decrements the module refcount, but the update path doesn't increment it. To avoid special-casing the update object release, do module_get for the update case too and release it via nft_obj_destroy(). **CVE ID: CVE-2022-48933**		
Affected Version(s): From (including) 5.4.61 Up to (excluding) 5.4.229					
NULL Pointer Dereference	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: efi: fix NULL-deref in init error path In cases where runtime services are not supported or have been disabled, the runtime services workqueue will	https://git.kernel.org/stable/c/4ca71bc0e1995d15486cd7b60845602a28399cb5, https://git.kernel.org/stable/c/585a0b2b3ae7903c6abee3087d09c69e955a7794, https://git.kernel.org/stable/c/5fcf75a8a4c3e7ee9122d143684083c9faf20452	O-LIN-LINU-030924/1293

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			never have been allocated. Do not try to destroy the workqueue unconditionally in the unlikely event that EFI initialisation fails to avoid dereferencing a NULL pointer. **CVE ID: CVE-2022-48879**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.103					
N/A	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response	https://git.kernel.org/stable/c/33222d1571d7ce8c1c75f6b488f38968fa93d2d9, https://git.kernel.org/stable/c/4ce247af3f30078d5b97554f1ae6200a0222c15a, https://git.kernel.org/stable/c/669c2b178956718407af5631ccbc61c24413f038	O-LIN-LINU-030924/1294

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/ rndis_get_next_response to prevent any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption. next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_givebac		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			k_request+0x20/0xe4 [361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979] dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1: irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c **CVE ID: CVE-2022-48926**		
Missing Release of Memory after	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2e798814e01827871938ff172d2b2ccf1e74b3	O-LIN-LINU-030924/1295

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			thermal: int340x: fix memory leak in int3400_notify() It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies 4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65 NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b 6b 6b 6b a5 rmal.kkkkkkkkkk. backtrace: [<ffffffff9c502c3e>] __kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0	55, https://git.kernel.org/stable/c/33c73a4d7e7b19313a6b417152f5365016926418, https://git.kernel.org/stable/c/3abea10e6a8f0e7804ed4c124bea2d15aca977c8	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff9c7b7d6e>] kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>] acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0 [<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0 [<ffffffff9c2cb4dd>] kthread+0xfd/0x130 [<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2022-48924		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function. **CVE ID: CVE-2022-48928**	https://git.kernel.org/stable/c/0f88722313645a903f4d420ba61ddc690ec2481d, https://git.kernel.org/stable/c/1aa12ecfdcbafebc218910ec47acf6262e600cf5, https://git.kernel.org/stable/c/53d43a9c8dd224e66559fe86af1e473802c7130e	O-LIN-LINU-030924/1296
Improper Locking	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing	https://git.kernel.org/stable/c/081bdc9fe05bb23248f5effb6f811da3da4b8252, https://git.kernel.org/stable/c/4752fafb461821f8c8581090c923ababba68c5bd, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1297

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync() **CVE ID: CVE-2022-48930**	8cc342508f9e7fdccd2e9758ae9d52aff72dab7f	
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix memory leak during stateful obj update stateful objects can be updated from the control plane. The transaction logic allocates a temporary object for this purpose. The ->init function was called for this object, so plain kfree() leaks resources. We must call ->destroy function of the object. nft_obj_destroy does this, but it also decrements the module refcount,	https://git.kernel.org/stable/c/34bb90e407e3288f610558beaae54ecaa32b11c4, https://git.kernel.org/stable/c/53026346a94c43f35c32b18804041bc483271d87, https://git.kernel.org/stable/c/7e9880e81d3fd6a43c202f205717485290432826	O-LIN-LINU-030924/1298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			but the update path doesn't increment it. To avoid special-casing the update object release, do module_get for the update case too and release it via nft_obj_destroy(). **CVE ID: CVE-2022-48933**		
Missing Release of Memory after Effective Lifetime	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: flower: Fix a potential leak in nfp_tunnel_add_shared_mac() ida_simple_get() returns an id between min (0) and max (NFP_MAX_MAC_INDEX) inclusive. So NFP_MAX_MAC_INDEX (0xff) is a valid id. In order for the error handling path to work correctly, the 'invalid'	https://git.kernel.org/stable/c/3a14d0888eb4b0045884126acc69abfb7b87814d, https://git.kernel.org/stable/c/4086d2433576baf85f0e538511df97c8101e0a10, https://git.kernel.org/stable/c/5ad5886f85b6bd893e3ed19013765fb0c243c069	O-LIN-LINU-030924/1299

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value for 'ida_idx' should not be in the 0..NFP_MAX_MAC_INDEX range, inclusive. So set it to -1. **CVE ID: CVE-2022-48934**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Aug-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is: A --> B --> C --> D	https://git.kernel.org/stable/c/3aadfd46858b1f64d4d6a0654b863e21aabff975, https://git.kernel.org/stable/c/40805099af11f68c5ca7dbcfacf455da8f99f622, https://git.kernel.org/stable/c/84ec758fb2daa236026506868c8796b0500c047d	O-LIN-LINU-030924/1300

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A <-- B <-- C <-- D delete list_head *B | delete list_head *C --------------------------------|----------------------------------- configfs_unregister_subsystem | configfs_unregister_subsystem unlink_group | unlink_group unlink_obj | unlink_obj list_del_init | list_del_init __list_del_entry | __list_del_entry __list_del | __list_del // next == C | next->prev = prev | | next->prev = prev prev->next = next | | // prev == B | prev->next = next Fix this by adding mutex when calling		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			link_group() or unlink_group(), but parent configfs_subsystem is NULL when config_item is root. So I create a mutex configfs_subsystem _mutex. **CVE ID: CVE-2022-48931**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.104					
Use After Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: fix use-after-free in __nf_register_net_hook() We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in	https://git.kernel.org/stable/c/05f7927b25d2635e87267ff6c79db79fb46cf313, https://git.kernel.org/stable/c/49c24579cec41e32f13d57b337fd28fb208d4a5b, https://git.kernel.org/stable/c/56763f12b0f02706576a088e85ef856deacc98a0	O-LIN-LINU-030924/1301

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430 CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #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		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.cold+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0 net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline] find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084 __sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xba/0x150 net/socket.c:2188 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: 0033:0x7f65a1ace7d9		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 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 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9 RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000 </TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993 prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35a/0x4a0 mm/slub. ---truncated--- **CVE ID: CVE-2022-48912**		
Double Free	22-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in	https://git.kernel.org/stable/c/147a0e71ccf96df9fc8c2ac500829d8e423ef02c, https://git.kernel.org/stable/c/2fe0e281f7ad0a62259649764228227dd6b2561d, https://git.kernel.org/stable/c/3d6cc9898efdfb062efb74dc18cfc700e082f5d5	O-LIN-LINU-030924/1302

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rcu_cblist_dequeue +0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4 [Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0 +0x24/0x150		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0 [Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0 ... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	__kasan_slab_free+0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae **CVE ID: CVE-2022-48919**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.198					
Use After Free	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unregister flowtable hooks on netns exit Unregister flowtable hooks before they are releases via	https://git.kernel.org/stable/c/6069da443bf65f513bb507bb21e2f87cfb1ad0b6 , https://git.kernel.org/stable/c/88c795491bf45a8c08a0f94c9ca4f13722e51013 , https://git.kernel.org/stable/c/8ffb8ac344884	O-LIN-LINU-030924/1303

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nf_tables_flowtable_destroy() otherwise hook core reports UAF. BUG: KASAN: use-after-free in nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 Read of size 4 at addr ffff8880736f7438 by task syz-executor579/3666 CPU: 0 PID: 3666 Comm: syz-executor579 Not tainted 5.16.0-rc5-syzkaller #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 lib/dump_stack.c:88 [inline]	5f65634889b051bd65e4dee484b	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lib/dump_stack.c:106 dump_stack_lvl+0x1dc/0x2d8 lib/dump_stack.c:106 lib/dump_stack.c:106 print_address_description+0x65/0x380 mm/kasan/report.c:247 mm/kasan/report.c:247 __kasan_report mm/kasan/report.c:433 [inline] __kasan_report mm/kasan/report.c:433 [inline] mm/kasan/report.c:450 kasan_report+0x19a/0x1f0 mm/kasan/report.c:450 mm/kasan/report.c:450 nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 __nf_register_net_hook+0x27e/0x8d0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netfilter/core.c:429 net/netfilter/core.c:429 nf_register_net_hook+0xaa/0x180 net/netfilter/core.c:571 net/netfilter/core.c:571 nft_register_flowtable_net_hooks+0x3c5/0x730 net/netfilter/nf_tables_api.c:7232 net/netfilter/nf_tables_api.c:7232 nf_tables_newflowtable+0x2022/0x2cf0 net/netfilter/nf_tables_api.c:7430 net/netfilter/nf_tables_api.c:7430 nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] net/netfilter/nfnetlink.c:652		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv+0x10e6/0x2550 net/netfilter/nfnetlink.c:652 net/netfilter/nfnetlink.c:652 __nft_release_hook() calls nft_unregister_flowtable_net_hooks() which only unregisters the hooks, then after RCU grace period, it is guaranteed that no packets add new entries to the flowtable (no flow offload rules and flowtable hooks are reachable from packet path), so it is safe to call nf_flow_table_free() which cleans up the remaining entries from the flowtable (both software and hardware) and it unbinds		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the flow_block. **CVE ID: CVE-2022-48935**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.224					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	O-LIN-LINU-030924/1304

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for sock_owned_by_user() and corresponding handling is missing. Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv. **CVE ID: CVE-2024-42271**		
Improper Check for Unusual or Exceptional Conditions	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return	https://git.kernel.org/stable/c/253405541be2f15ffebdeac2f4cf4b7e9144d12f, https://git.kernel.org/stable/c/2abe350db1aa599eeebc6892237d0bce0f1de62a, https://git.kernel.org/stable/c/5eea127675450	O-LIN-LINU-030924/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address. **CVE ID: CVE-2024-42284**	583680c8170358bcba43227bd69	

Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:
			RDMA/iwcm: Fix a use-after-free related to destroying CM IDs
			iw_conn_req_handler() associates a new struct rdma_id_private (conn_id) with
			an existing struct iw_cm_id (cm_id) as follows:
			conn_id->cm_id.iw = cm_id;
			cm_id->context = conn_id;
			cm_id->cm_handler = cma_iw_handler;
				https://git.kernel.org/stable/c/557d035fe88d78dd51664f4dc0e1896c04c97cf6, https://git.kernel.org/stable/c/7f25f296fc9bd0435be14e89bf657cd615a23574, https://git.kernel.org/stable/c/94ee7ff99b87435ec63211f632918dc7f44dac79	O-LIN-LINU-030924/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdma_destroy_id() frees both the cm_id and the struct rdma_id_private. Make sure that cm_work_handler() does not trigger a use-after-free by only freeing of the struct rdma_id_private after all pending work has finished. **CVE ID: CVE-2024-42285**		
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered	https://git.kernel.org/stable/c/166a0bddcc27de41fe13f861c8348e8e53e988c8, https://git.kernel.org/stable/c/47b3dce100778001cd76f7e9188944b5cb27a76d, https://git.kernel.org/stable/c/7789a1d6792af410aa9b39a1eb237ed24fa2170a	O-LIN-LINU-030924/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QThread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dump_backtrace+0x0/0x1c0 [66.575469s] [pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s] [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport] **CVE ID: CVE-2024-42301**		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close	https://git.kernel.org/stable/c/4c9d235630d35db762b85a4149bbb0be9d504c36, https://git.kernel.org/stable/c/66fa52edd32cdbb675f0803b3c4da10ea19b6635,	O-LIN-LINU-030924/1308

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decoding can incur a read after free for inst. Fix it by cancelling the work in vdec_close. **CVE ID: CVE-2024-42313**	https://git.kernel.org/stable/c/6a96041659e834dc0b172dda4b2df512d63920c2	
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree **CVE ID: CVE-2024-43858**	https://git.kernel.org/stable/c/538a27c8048f081a5ddd286f886eb986fbbc7f80, https://git.kernel.org/stable/c/55b732c8b09b41148eaab2fa8e31b0af47671e00, https://git.kernel.org/stable/c/63f7fdf733add8	O-LIN-LINU-030924/1309

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2f126ea00e2e48f6eba15ac4b9	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed when receiving ICMP packets with secmark set while an ICMP raw socket is being created. SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socket before that, causing the null pointer dereference. Drop the packet if label context is not set. BUG: kernel NULL pointer dereference, address:	https://git.kernel.org/stable/c/0abe35bc48d4ec80424b1f4b3560c0e082cbd5c1, https://git.kernel.org/stable/c/290a6b88e8c19b6636ed1acc733d1458206f7697, https://git.kernel.org/stable/c/347dcb84a4874b5fb375092c08d8cc4069b94f81	O-LIN-LINU-030924/1310

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			000000000000004c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1 3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 RIP: 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 89 f0 <8b> 77 4c 39 c6 7e 1f 48 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 000000000000000e RDX: ffffa92940003be8 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400 R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 R12: ffff8b574c642400 R13: 0000000000000001 R14: 0000000000000001 R15: 0000000000000000 FS: 00007fb092ea7640(0000) GS:ffff8b577bc000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40 apparmor_secmark_check+0xec/0x330 security_sock_rcv_skb+0x35/0x50		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0 ip_local_deliver_finish+0x76/0xa0 __netif_receive_skb_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 net_rx_action+0x2a4/0x380 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0 common_interrupt+0x86/0xa0 </IRQ> <TASK> asm_common_interrupt+0x26/0x40 RIP: 0010:apparmor_socket_post_create+0xb/0x200 Code: 08 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00 00 48 8b 1d 80 56 3f 02 48 RSP: 0018:ffffa92940ce		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000002 RDI: ffff8b574eaab740 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 0000000000000002 R14: ffff8b574eaab740 R15: ffffffffbd8e4748 ? __pfx_apparmor_socket_post_create+0x10/0x10 security_socket_po		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			st_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys_socket+0x89/0x100 __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc **CVE ID: CVE-2023-52889**		
Use of Uninitialized Resource	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: Initialize all fields in dumped nexthops	https://git.kernel.org/stable/c/1377de719652d868f5317ba8398b7e74c5f0430b, https://git.kernel.org/stable/c/5cc4d71dda2dd4f1520f40e634a527022e48ccd8,	O-LIN-LINU-030924/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	struct nexthop_grp contains two reserved fields that are not initialized by nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity): # ip nexthop add id 1 dev lo # ip nexthop add id 101 group 1 # strace -e recvmsg ip nexthop get id 101 ... recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52 The fields are reserved and therefore not currently used. But as they are, they leak kernel memory, and the fact they are not just zero	https://git.kernel.org/stable/c/6d745cd0e9720282cd291d36b9db528aea18add2	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			complicates repurposing of the fields for new ends. Initialize the full structure. **CVE ID: CVE-2024-42283**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes In psb_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42309**	https://git.kernel.org/stable/c/13b5f3ee94bdbdc4b5f40582aab62977905aedee, https://git.kernel.org/stable/c/2df7aac81070987b0f052985856aa325a38debf6, https://git.kernel.org/stable/c/46d2ef272957879cbe30a884574320e7f7d78692	O-LIN-LINU-030924/1312
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/08f45102c81ad8bc9f85f7a25e9f64e128edb87d,	O-LIN-LINU-030924/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42310**	https://git.kernel.org/stable/c/2d209b2f862f6b8bff549ede541590a8d119da23, https://git.kernel.org/stable/c/977ee4fe895e1729cd36cc26916bbb10084713d6	
Allocation of Resources Without Limits or Throttling	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse,	https://git.kernel.org/stable/c/1fe97f68fce1ba24bf823bfb0eb0956003473130, https://git.kernel.org/stable/c/22094f5f52e7bc16c5bf9613365049383650b02e, https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7	O-LIN-LINU-030924/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list. If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ac2f-a84d81075b03 **CVE ID: CVE-2024-43856**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node value is NULL In imx_rproc_addr_init() "nph = of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE.	https://git.kernel.org/stable/c/2fa26ca8b786888673689ccc9da6094150939982, https://git.kernel.org/stable/c/4e13b7c23988c0a13fdca92e94296a3bc2ff9f21, https://git.kernel.org/stable/c/6884fd0283e0831be153fb8d82d9eda8a55acaaa	O-LIN-LINU-030924/1315

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Fixed title to fit within the prescribed 70-75 charcters] **CVE ID: CVE-2024-43860**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer dereference to ras_manager Check ras_manager before using it **CVE ID: CVE-2024-43908**	https://git.kernel.org/stable/c/033187a70ba9743c73a810a006816e5553d1e7d4, https://git.kernel.org/stable/c/48cada0ac79e4775236d642e9ec5998a7c7fb7a4, https://git.kernel.org/stable/c/4c11d30c95576937c6c35e6f29884761f2dddb43	O-LIN-LINU-030924/1316
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in	https://git.kernel.org/stable/c/05e4a0fa248240efd99a539853e844f0f0a9e6a5 , https://git.kernel.org/stable/c/1407be30fc17eff918a98e0a990c0e988f11dc84, https://git.kernel.org/stable/c/52319d9d2f522ed939af31af70f8c3a0f0f67e6c	O-LIN-LINU-030924/1317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_sock() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock().		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint(). [0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89 f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0 R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated--- **CVE ID: CVE-2024-44935**		
Affected Version(s): From (including) 5.6 Up to (excluding) 5.10.103					
Excessive Iteration	22-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: bpf: Add schedule points in batch ops	https://git.kernel.org/stable/c/75134f16e7dd0007aa474b281935c5f42e79f2c8, https://git.kernel.org/stable/c/7e8099967d0e3ff9d1ae043e8	O-LIN-LINU-030924/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syzbot reported various soft lockups caused by bpf batch operations. INFO: task kworker/1:1:27 blocked for more than 140 seconds. INFO: task hung in rcu_barrier Nothing prevents batch ops to process huge amount of data, we need to add schedule points in them. Note that maybe_wait_bpf_programs(map) calls from generic_map_delete_batch() can be factorized by moving the call after the loop. This will be done later in -next tree once we get this fix merged, unless there is strong opinion doing this	0b27fbe46c08417, https://git.kernel.org/stable/c/7ef94bfb08fb9e73defafbd5ddef6b5a0e2ee12b	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			optimization sooner. **CVE ID: CVE-2022-48939**		
Affected Version(s): From (including) 5.7 Up to (excluding) 5.10.103					
Improper Locking	22-Aug-2024	3.3	In the Linux kernel, the following vulnerability has been resolved: io_uring: add a schedule point in io_add_buffers() Looping ~65535 times doing kmalloc() calls can trigger soft lockups, especially with DEBUG features (like KASAN). [253.536212] watchdog: BUG: soft lockup - CPU#64 stuck for 26s! [b219417889:12575] [253.544433] Modules linked in: vfat fat i2c_mux_pca954x i2c_mux spidev cdc_acm xhci_pci xhci_hcd sha3_generic gq(O) [253.544451] CPU: 64 PID: 12575 Comm:	https://git.kernel.org/stable/c/4a93c6594613c3429b6f30136fff115c7f803af4, https://git.kernel.org/stable/c/8f3cc3c5bc43d03b5748ac4fb8d180084952c36a, https://git.kernel.org/stable/c/c718ea4e7382e18957ed0e88a5f855e2122d9c00	O-LIN-LINU-030924/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			b219417889 Tainted: G S O 5.17.0-smp-DEV #801 [253.544457] RIP: 0010:kernel_text_address (./include/asm-generic/sections.h:192 ./include/linux/kallsyms.h:29 kernel/extable.c:67 kernel/extable.c:98) [253.544464] Code: 0f 93 c0 48 c7 c1 e0 63 d7 a4 48 39 cb 0f 92 c1 20 c1 0f b6 c1 5b 5d c3 90 0f 1f 44 00 00 55 48 89 e5 41 57 41 56 53 48 89 fb <48> c7 c0 00 00 80 a0 41 be 01 00 00 00 48 39 c7 72 0c 48 c7 c0 40 [253.544468] RSP: 0018:ffff8882d8baf4c0 EFLAGS: 00000246 [253.544471] RAX: 1ffff1105b175e00 RBX: ffffffffa13ef09a RCX: 00000000a13ef001 [253.544474] RDX: ffffffffa13ef09a RSI:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff8882d8baf558 RDI: ffffffffa13ef09a [253.544476] RBP: ffff8882d8baf4d8 R08: ffff8882d8baf5e0 R09: 0000000000000004 [253.544479] R10: ffff8882d8baf5e8 R11: ffffffffa0d59a50 R12: ffff8882eab20380 [253.544481] R13: ffffffffa0d59a50 R14: dffffc0000000000 R15: 1ffff1105b175eb0 [253.544483] FS: 00000000016d3380(0000) GS:ffff88af48c00000(0000) knlGS:0000000000000000 [253.544486] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [253.544488] CR2: 00000000004af0f0 CR3: 00000002eabfa004 CR4: 00000000003706e0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[253.544491] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [253.544492] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [253.544494] Call Trace: [253.544496] <TASK> [253.544498] ? io_queue_sqe (fs/io_uring.c:7143) [253.544505] __kernel_text_address (kernel/extable.c:78) [253.544508] unwind_get_return_address (arch/x86/kernel/unwind_frame.c:19) [253.544514] arch_stack_walk (arch/x86/kernel/stacktrace.c:27) [253.544517] ? io_queue_sqe		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(fs/io_uring.c:7143) [253.544521] stack_trace_save (kernel/stacktrace.c:123) [253.544527] ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544531] ? ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544533] ? __kasan_kmalloc (mm/kasan/common.c:524) [253.544535] ? kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544541] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828)		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[253.544544] ? __io_queue_sqe (fs/io_uring.c:?) [253.544551] __kasan_kmalloc (mm/kasan/common.c:524) [253.544553] kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544556] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544560] io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544564] ? __kasan_slab_alloc (mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544567] ? __kasan_slab_alloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[253.544569] ? kmem_cache_alloc_bulk (mm/slab.h:732 mm/slab.c:3546) [253.544573] ? __io_alloc_req_refill (fs/io_uring.c:2078) [253.544578] ? io_submit_sqes (fs/io_uring.c:7441) [253.544581] ? __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uring.c:10096) [253.544584] ? __x64_sys_io_uring_enter (fs/io_uring.c:10096) [253.544587] ? do_syscall_64 (arch/x86/entry/common.c:50 arch/x86/entry/common.c:80) [253.544590] ? entry_SYSCALL_64_after_hwframe (??:?) [253.544596] __io_queue_sqe (fs/io_uring.c:?) [253.544600] io_queue_sqe		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(fs/io_uring.c:7143) [253.544603] io_submit_sqe (fs/io_uring.c:?) [253.544608] io_submit_sqes (fs/io_uring.c:?) [253.544612] __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uri ---truncated--- **CVE ID: CVE-2022-48937**		
Affected Version(s): From (including) 5.8 Up to (excluding) 5.10.103					
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: hwmon: Handle failure to register sensor with thermal zone correctly If an attempt is made to a sensor with a thermal zone and it fails, the call to devm_thermal_zone_of_sensor_register() may return -ENODEV.	https://git.kernel.org/stable/c/1b5f517cca36292076d9e38fa6e33a257703e62e, https://git.kernel.org/stable/c/7efe8499cb90651c540753f4269d2d43ede14223, https://git.kernel.org/stable/c/8a1969e14ad93663f9a3ed02ccc2138da9956a0e	O-LIN-LINU-030924/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This may result in crashes similar to the following. Unable to handle kernel NULL pointer dereference at virtual address 00000000000003cd ... Internal error: Oops: 96000021 [#1] PREEMPT SMP ... pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : mutex_lock+0x18/0x60 lr : thermal_zone_device_update+0x40/0x2e0 sp : ffff800014c4fc60 x29: ffff800014c4fc60 x28: ffff365ee3f6e000 x27: ffffdde218426790 x26: ffff365ee3f6e000 x25: 000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 x24: ffff365ee3f6e000 x23: ffffdde218426870 x22: ffff365ee3f6e000 x21: 00000000000003cd x20: ffff365ee8bf3308 x19: ffffffffffffffed x18: 0000000000000000 x17: ffffdde21842689c x16: ffffdde1cb7a0b7c x15: 0000000000000040 x14: ffffdde21a4889a0 x13: 0000000000000228 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000000001120000 x7 : 0000000000000001 x6 :		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 x5 : 0068000878e20f07 x4 : 0000000000000000 x3 : 00000000000003cd x2 : ffff365ee3f6e000 x1 : 0000000000000000 x0 : 00000000000003cd Call trace: mutex_lock+0x18/0x60 hwmon_notify_event+0xfc/0x110 0xffffdde1cb7a0a90 0xffffdde1cb7a0b7c irq_thread_fn+0x2c/0xa0 irq_thread+0x134/0x240 kthread+0x178/0x190		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ret_from_fork+0x10/0x20 Code: d503201f d503201f d2800001 aa0103e4 (c8e47c02) Jon Hunter reports that the exact call sequence is: hwmon_notify_event() --> hwmon_thermal_notify() --> thermal_zone_device_update() --> update_temperature() --> mutex_lock() The hwmon core needs to handle all errors returned from calls to devm_thermal_zone_of_sensor_register(). If the call fails with -ENODEV, report that the sensor was not attached to a		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thermal zone but continue to register the hwmon device. **CVE ID: CVE-2022-48942**		
Affected Version(s): From (including) 5.8 Up to (excluding) 5.10.165					
Use After Free	21-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_qca: Fix driver shutdown on closed serdev The driver shutdown callback (which sends EDL_SOC_RESET to the device over serdev) should not be invoked when HCI device is not open (e.g. if hci_dev_open_sync() failed), because the serdev and its TTY are not open either. Also skip this step if device is powered off (qca_power_shutdown()). The shutdown callback causes use-after-free	https://git.kernel.org/stable/c/272970be3dabd24cbe50e393ffee8f04aec3b9a8, https://git.kernel.org/stable/c/908d1742b6e694e84ead5c62e4b7c1bfbb8b46a3, https://git.kernel.org/stable/c/e84ec6e25df9bb0968599e92eacedaf3a0a5b587	O-LIN-LINU-030924/1321

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during system reboot with Qualcomm Atheros Bluetooth: Unable to handle kernel paging request at virtual address 0072662f67726fd7 ... CPU: 6 PID: 1 Comm: systemd-shutdow Tainted: G W 6.1.0-rt5-00325-g8a5f56bcfcca #8 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace: tty_driver_flush_buffer+0x4/0x30 serdev_device_write_flush+0x24/0x34 qca_serdev_shutdown+0x80/0x130 [hci_uart] device_shutdown+0x15c/0x260 kernel_restart+0x48/0xac		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KASAN report: BUG: KASAN: use-after-free in tty_driver_flush_buffer+0x1c/0x50 Read of size 8 at addr ffff16270c2e0018 by task systemd-shutdow/1 CPU: 7 PID: 1 Comm: systemd-shutdow Not tainted 6.1.0-next-20221220-00014-gb85aaf97fb01-dirty #28 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace: dump_backtrace.part.0+0xdc/0xf0 show_stack+0x18/0x30 dump_stack_lvl+0x68/0x84 print_report+0x188/0x488		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_report+0xa4/0xf0 __asan_load8+0x80/0xac tty_driver_flush_buffer+0x1c/0x50 ttyport_write_flush+0x34/0x44 serdev_device_write_flush+0x48/0x60 qca_serdev_shutdown+0x124/0x274 device_shutdown+0x1e8/0x350 kernel_restart+0x48/0xb0 __do_sys_reboot+0x244/0x2d0 __arm64_sys_reboot+0x54/0x70 invoke_syscall+0x60/0x190 el0_svc_common.constprop.0+0x7c/0x160 do_el0_svc+0x44/0xf0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			el0_svc+0x2c/0x6c el0t_64_sync_handler+0xbc/0x140 el0t_64_sync+0x190/0x194 **CVE ID: CVE-2022-48878**		
Affected Version(s): From (including) 5.8 Up to (excluding) 5.10.224					
Divide By Zero	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time. [10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1	https://git.kernel.org/stable/c/6d45e1c948a8b7ed6ceddb14319af69424db730c, https://git.kernel.org/stable/c/8f5ffd2af7274853ff91d6cd62541191d9fbd10d, https://git.kernel.org/stable/c/924f788c906dccaca30acab86c7124371e1d6f2c	O-LIN-LINU-030924/1322

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021 [10.017908] Workqueue: events_unbound padata_mt_helper [10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 : [10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330 [10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[10.018147] </TASK> Looking at the padata_mt_helper() function, the only way a divide-by-0 panic can happen is when ps->chunk_size is 0. The way that chunk_size is initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least 1 no matter what the input parameters are. **CVE ID: CVE-2024-43889**		
Affected Version(s): From (including) 5.9 Up to (excluding) 5.10.104					
NULL Pointer Dereference	22-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: core: Fix TZ_GET_TRIP NULL	https://git.kernel.org/stable/c/1c0b51e62a50e9291764d022ed44549e65d6ab9c, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1323

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference Do not call get_trip_hyst() from thermal_genl_cmd_tz_get_trip() if the thermal zone does not define one. **CVE ID: CVE-2022-48915**	3dafbf915c05f83469e791949b5590da2aca2afb, https://git.kernel.org/stable/c/4c294285cec3964b3291772ac0642c2bf440bd1b	
Affected Version(s): From (including) 5.9 Up to (excluding) 5.10.164					
NULL Pointer Dereference	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: efi: fix NULL-deref in init error path In cases where runtime services are not supported or have been disabled, the runtime services workqueue will never have been allocated. Do not try to destroy the workqueue unconditionally in the unlikely event that EFI initialisation fails to	https://git.kernel.org/stable/c/4ca71bc0e1995d15486cd7b60845602a28399cb5, https://git.kernel.org/stable/c/585a0b2b3ae7903c6abee3087d09c69e955a7794, https://git.kernel.org/stable/c/5fcf75a8a4c3e7ee9122d143684083c9faf20452	O-LIN-LINU-030924/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			avoid dereferencing a NULL pointer. **CVE ID: CVE-2022-48879**		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.1.104					
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix missing lock on sync reset reload On sync reset reload work, when remote host updates devlink on reload actions performed on that host, it misses taking devlink lock before calling devlink_remote_reload_actions_performed() which results in triggering lock assert like the following: WARNING: CPU: 4 PID: 1164 at net/devlink/core.c: 261	https://git.kernel.org/stable/c/091268f3c27a5b6d7858a3bb2a0dbcc9cd26ddb5, https://git.kernel.org/stable/c/572f9caa9e7295f8c8822e4122c7ae8f1c412ff9, https://git.kernel.org/stable/c/5d07d1d40aabfd61bab21115639bd4f641db6002	O-LIN-LINU-030924/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devl_assert_locked+0x3e/0x50 ... CPU: 4 PID: 1164 Comm: kworker/u96:6 Tainted: G S W 6.10.0-rc2+ #116 Hardware name: Supermicro SYS-2028TP-DECTR/X10DRT-PT, BIOS 2.0 12/18/2015 Workqueue: mlx5_fw_reset_events mlx5_sync_reset_reload_work [mlx5_core] RIP: 0010:devl_assert_locked+0x3e/0x50 ... Call Trace: <TASK> ? __warn+0xa4/0x210 ? devl_assert_locked+0x3e/0x50 ? report_bug+0x160/0x280 ? handle_bug+0x3f/0x80		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? exc_invalid_op+0x17/0x40 ? asm_exc_invalid_op+0x1a/0x20 ? devl_assert_locked+0x3e/0x50 devlink_notify+0x88/0x2b0 ? mlx5_attach_device+0x20c/0x230 [mlx5_core] ? __pfx_devlink_notify+0x10/0x10 ? process_one_work+0x4b6/0xbb0 process_one_work+0x4b6/0xbb0 […] **CVE ID: CVE-2024-42268**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.103					
Divide By Zero	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/mglru: fix div-by-zero in vmpressure_calc_level()	https://git.kernel.org/stable/c/8b671fe1a879923ecfb72dda6caf01460dd885ef, https://git.kernel.org/stable/c/8de7bf77f21068a5f602bb1e59adbc5ab533509	O-LIN-LINU-030924/1326

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			evict_folios() uses a second pass to reclaim folios that have gone through page writeback and become clean before it finishes the first pass, since folio_rotate_reclaimable() cannot handle those folios due to the isolation. The second pass tries to avoid potential double counting by deducting scan_control->nr_scanned. However, this can result in underflow of nr_scanned, under a condition where shrink_folio_list() does not increment nr_scanned, i.e., when folio_trylock() fails. The underflow can cause the divisor, i.e., scale=scanned+reclaimed in vmpressure_calc_level(), to become	d, https://git.kernel.org/stable/c/a39e38be632f0e1c908d70d1c9cd071c03faf895	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			zero, resulting in the following crash: [exception RIP: vmpressure_work_fn+101] process_one_work at ffffffffa3313f2b Since scan_control->nr_scanned has no established semantics, the potential double counting has minimal risks. Therefore, fix the problem by not deducting scan_control->nr_scanned in evict_folios(). **CVE ID: CVE-2024-42316**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.7					
NULL Pointer Dereference	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix macsec possible null dereference when updating MAC security entity (SecY) Upon updating MAC security entity	https://git.kernel.org/stable/c/514d9c6a39213d8200884e70f60ce7faef1ee597, https://git.kernel.org/stable/c/9828994ac492e8e7de47fe66097b7e665328f348	O-LIN-LINU-030924/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SecY) in hw offload path, the macsec security association (SA) initialization routine is called. In case of extended packet number (epn) is enabled the salt and ssci attributes are retrieved using the MACsec driver rx_sa context which is unavailable when updating a SecY property such as encoding-sa hence the null dereference. Fix by using the provided SA to set those attributes. **CVE ID: CVE-2022-48882**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.8					
NULL Pointer Dereference	21-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix initialization of rx->link and rx->link_sta There are some codepaths that do	https://git.kernel.org/stable/c/a57c981d9f24d2bd89eaa76dc477e8ca252e22e8, https://git.kernel.org/stable/c/e66b7920aa5ac5b1a1997a454004ba9246a3c005	O-LIN-LINU-030924/1328

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not initialize rx->link_sta properly. This causes a crash in places which assume that rx->link_sta is valid if rx->sta is valid. One known instance is triggered by __ieee80211_rx_h_amsdu being called from fast-rx. It results in a crash like this one: BUG: kernel NULL pointer dereference, address: 00000000000000a8 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: 0002 [#1] PREEMPT SMP PTI CPU: 1 PID: 506 Comm: mt76-usb-rx phy Tainted: G E 6.1.0-debian64x+1.7 #3		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: ZOTAC ZBOX-ID92/ZBOX-IQ01/ZBOX-ID92/ZBOX-IQ01, BIOS B220P007 05/21/2014 RIP: 0010:ieee80211_deliver_skb+0x62/0x1f0 [mac80211] Code: 00 48 89 04 24 e8 9e a7 c3 df 89 c0 48 03 1c c5 a0 ea 39 a1 4c 01 6b 08 48 ff 03 48 83 7d 28 00 74 11 48 8b 45 30 48 63 55 44 <48> 83 84 d0 a8 00 00 00 01 41 8b 86 c0 11 00 00 8d 50 fd 83 fa 01 RSP: 0018:ffff999040803b10 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffffb9903f496480 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: ffff999040803ce0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff8d21828ac900 R13: 000000000000004a R14: ffff8d2198ed89c0 R15: ffff8d2198ed8000 FS: 0000000000000000(0000) GS:ffff8d24afe80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000000000a8 CR3: 0000000429810002 CR4: 00000000001706e0 Call Trace: <TASK> __ieee80211_rx_h_a		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			msdu+0x1b5/0x240 [mac80211] ? ieee80211_prepare_and_rx_handle+0xcdd/0x1320 [mac80211] ? __local_bh_enable_ip+0x3b/0xa0 ieee80211_prepare_and_rx_handle+0xcdd/0x1320 [mac80211] ? prepare_transfer+0x109/0x1a0 [xhci_hcd] ieee80211_rx_list+0xa80/0xda0 [mac80211] mt76_rx_complete+0x207/0x2e0 [mt76] mt76_rx_poll_complete+0x357/0x5a0 [mt76] mt76u_rx_worker+0x4f5/0x600 [mt76_usb] ? mt76_get_min_avg_rssi+0x140/0x140 [mt76]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__mt76_worker_fn+0x50/0x80 [mt76] kthread+0xed/0x120 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x22/0x30 Since the initialization of rx->link and rx->link_sta is rather convoluted and duplicated in many places, clean it up by using a helper function to set it. [remove unnecessary rx->sta->sta.mlo check] **CVE ID: CVE-2022-48876**		
Affected Version(s): From (including) 6.10 Up to (excluding) 6.10.3					
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: mediatek: Fix potential NULL	https://git.kernel.org/stable/c/16f3a28cf5f876a7f3550d8f4c870a7b41bcfaef, https://git.kernel.org/stable/c/af6bd5c9901b1	O-LIN-LINU-030924/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference in dummy net_device handling Move the freeing of the dummy net_device from mtk_free_dev() to mtk_remove(). Previously, if alloc_netdev_dummy() failed in mtk_probe(), eth->dummy_dev would be NULL. The error path would then call mtk_free_dev(), which in turn called free_netdev() assuming dummy_dev was allocated (but it was not), potentially causing a NULL pointer dereference. By moving free_netdev() to mtk_remove(), we ensure it's only called when mtk_probe() has succeeded and dummy_dev is fully allocated. This	3a26eaf4d57d97a813297791596	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses a potential NULL pointer dereference detected by Smatch[1]. **CVE ID: CVE-2024-42282**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: ethtool: pse-pd: Fix possible null-deref Fix a possible null dereference when a PSE supports both c33 and PoDL, but only one of the netlink attributes is specified. The c33 or PoDL PSE capabilities are already validated in the ethnl_set_pse_validate() call. **CVE ID: CVE-2024-43836**	https://git.kernel.org/stable/c/4cddb0f15ea9c62f81b4889ea69a99368cc63a86, https://git.kernel.org/stable/c/e187690b125a297499eadeec53c32c5ed6d7436a	O-LIN-LINU-030924/1330
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.44					
Improper Check for Unusual or Exceptional Conditions	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from	https://git.kernel.org/stable/c/253405541be2f15ffebdeac2f4cf4b7e9144d12f, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1331

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tipc_udp_addr2str() on error tipc_udp_addr2str() should return non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address. **CVE ID: CVE-2024-42284**	2abe350db1aa599eeebc6892237d0bce0f1de62a, https://git.kernel.org/stable/c/5eea127675450583680c8170358bcba43227bd69	
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix a use-after-free related to destroying CM IDs iw_conn_req_handler() associates a new struct rdma_id_private (conn_id) with an existing struct iw_cm_id (cm_id) as follows: conn_id->cm_id.iw = cm_id;	https://git.kernel.org/stable/c/557d035fe88d78dd51664f4dc0e1896c04c97cf6, https://git.kernel.org/stable/c/7f25f296fc9bd0435be14e89bf657cd615a23574, https://git.kernel.org/stable/c/94ee7ff99b87435ec63211f632918dc7f44dac79	O-LIN-LINU-030924/1332

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			cm_id->context = conn_id;
			cm_id->cm_handler = cma_iw_handler;
			rdma_destroy_id() frees both the cm_id and the struct rdma_id_private. Make
			sure that cm_work_handler() does not trigger a use-after-free by only
			freeing of the struct rdma_id_private after all pending work has finished.
			CVE ID: CVE-2024-42285		

Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying,	https://git.kernel.org/stable/c/166a0bddcc27de41fe13f861c8348e8e53e988c8, https://git.kernel.org/stable/c/47b3dce100778001cd76f7e9188944b5cb27a76d, https://git.kernel.org/stable/c/7789a1d6792af410aa9b39a1eb237ed24fa2170a	O-LIN-LINU-030924/1333

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ensuring the destination buffer is not overflowed. Below is the stack trace I encountered during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QThread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9] dump_backtrace+0x0/0x1c0 [66.575469s] [pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s] [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport] **CVE ID: CVE-2024-42301**		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/11a1f4bc47362	O-LIN-LINU-030924/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a DPC event occurs concurrently to hot-removal of the same portion of the hierarchy: The dpc_handler() awaits readiness of the secondary bus below the Downstream Port where the DPC event occurred. To do so, it polls the config space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct pci_dev cause the kernel to oops. That's because pci_bridge_wait_for_secondary_bus() neglects to hold a	700fcbde717292158873fb847ed, https://git.kernel.org/stable/c/2c111413f38ca5cf87557cab89f6d82b0e3433e7, https://git.kernel.org/stable/c/2cc8973bdc4d6c928ebe38b88090a2cdfe81f42f	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reference on the child device. Before v6.3, the function was only called on resume from system sleep or on runtime resume. Holding a reference wasn't necessary back then because the pciehp IRQ thread could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the resume_noirq phase. And runtime resume is always awaited before a PCI device is removed.) However starting with v6.3, pci_bridge_wait_for_secondary_bus() is also called on a DPC event. Commit 53b54ad074de ("PCI/DPC: Await readiness of secondary bus after reset"), which introduced that, failed to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			appreciate that pci_bridge_wait_for_secondary_bus() now needs to hold a reference on the child device because dpc_handler() and pciehp may indeed run concurrently. The commit was backported to v5.10+ stable kernels, so that's the oldest one affected. Add the missing reference acquisition. Abridged stack trace: BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464 Comm: irq/53-pcie-dpc 6.9.0 RIP: pci_bus_read_config_dword+0x17/0x50 pci_dev_wait()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			pci_bridge_wait_for _secondary_bus()
			dpc_reset_link()
			pcie_do_recovery()
			dpc_handler()
			CVE ID: CVE-2024-42302		

Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decoding can incur a read after free for inst.	https://git.kernel.org/stable/c/4c9d235630d35db762b85a4149bbb0be9d504c36, https://git.kernel.org/stable/c/66fa52edd32cdbb675f0803b3c4da10ea19b6635, https://git.kernel.org/stable/c/6a96041659e834dc0b172dda4b2df512d63920c2	O-LIN-LINU-030924/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix it by cancelling the work in vdec_close. **CVE ID: CVE-2024-42313**		
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree **CVE ID: CVE-2024-43858**	https://git.kernel.org/stable/c/538a27c8048f081a5ddd286f886eb986fbbc7f80, https://git.kernel.org/stable/c/55b732c8b09b41148eaab2fa8e31b0af47671e00, https://git.kernel.org/stable/c/63f7fdf733add82f126ea00e2e48f6eba15ac4b9	O-LIN-LINU-030924/1336
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed when receiving ICMP packets with secmark set while an ICMP raw socket is being created.	https://git.kernel.org/stable/c/0abe35bc48d4ec80424b1f4b3560c0e082cbd5c1, https://git.kernel.org/stable/c/290a6b88e8c19b6636ed1acc733d1458206f7697, https://git.kernel.org/stable/c/347dcb84a4874b5fb375092c08d8cc4069b94f81	O-LIN-LINU-030924/1337

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socket before that, causing the null pointer dereference. Drop the packet if label context is not set. BUG: kernel NULL pointer dereference, address: 000000000000004c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1 3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 RIP: 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 89 f0 <8b> 77 4c 39 c6 7e 1f 48 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2 RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 000000000000000e RDX: ffffa92940003be8 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 R12: ffff8b574c642400 R13: 0000000000000001 R14: 0000000000000001 R15: 0000000000000000 FS: 00007fb092ea7640(0000) GS:ffff8b577bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40 apparmor_secmark_check+0xec/0x330 security_sock_rcv_skb+0x35/0x50 sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0 ip_local_deliver_finish+0x76/0xa0 __netif_receive_skb		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 net_rx_action+0x2a4/0x380 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0 common_interrupt+0x86/0xa0 </IRQ> <TASK>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			asm_common_interrupt+0x26/0x40 RIP: 0010:apparmor_socket_post_create+0xb/0x200 Code: 08 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00 00 48 8b 1d 80 56 3f 02 48 RSP: 0018:ffffa92940ce7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000002 RDI: ffff8b574eaab740 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 0000000000000002 R14: ffff8b574eaab740 R15: ffffffffbd8e4748 ? __pfx_apparmor_socket_post_create+0x10/0x10 security_socket_post_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys_socket+0x89/0x100 __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc **CVE ID: CVE-2023-52889**		
Use of Uninitialized Resource	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: Initialize all fields in dumped nexthops struct nexthop_grp contains two reserved fields that are not initialized by nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity): # ip nexthop add id 1 dev lo # ip nexthop add id 101 group 1 # strace -e recvmsg ip nexthop get id 101 ...	https://git.kernel.org/stable/c/1377de719652d868f5317ba8398b7e74c5f0430b, https://git.kernel.org/stable/c/5cc4d71dda2dd4f1520f40e634a527022e48ccd8, https://git.kernel.org/stable/c/6d745cd0e9720282cd291d36b9db528aea18add2	O-LIN-LINU-030924/1338

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52 The fields are reserved and therefore not currently used. But as they are, they leak kernel memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure. **CVE ID: CVE-2024-42283**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes In psb_intel_lvds_get_modes(), the return	https://git.kernel.org/stable/c/13b5f3ee94bdbdc4b5f40582aab62977905aedee, https://git.kernel.org/stable/c/2df7aac81070987b0f052985856aa325a38debf6, https://git.kernel.org/stable/c/46d2ef272957879cbe30a88457	O-LIN-LINU-030924/1339

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42309**	4320e7f7d78692	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	https://git.kernel.org/stable/c/08f45102c81ad8bc9f85f7a25e9f64e128edb87d, https://git.kernel.org/stable/c/2d209b2f862f6b8bff549ede541590a8d119da23, https://git.kernel.org/stable/c/977ee4fe895e1729cd36cc26916bbb10084713d6	O-LIN-LINU-030924/1340

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42310		
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: exfat: fix potential deadlock on __exfat_get_dentry_set When accessing a file with more entries than ES_MAX_ENTRY_NUM, the bh-array is allocated in __exfat_get_entry_set. The problem is that the bh-array is allocated with GFP_KERNEL. It does not make sense. In the following cases, a deadlock for sbi->s_lock between the two processes may occur. CPU0 CPU1 ---- ---- kswapd balance_pgdat lock(fs_reclaim) exfat_iterate	https://git.kernel.org/stable/c/1d1970493c289e3f44b9ec847ed26a5dbdf56a62, https://git.kernel.org/stable/c/89fc548767a2155231128cb98726d6d2ea1256c9, https://git.kernel.org/stable/c/a7ac198f8dba791e3144c4da48a5a9b95773ee4b	O-LIN-LINU-030924/1341

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lock(&sbi->s_lock) exfat_readdir exfat_get_uniname_from_ext_entry exfat_get_dentry_set __exfat_get_dentry_set kmalloc_array ... lock(fs_reclaim) ... evict exfat_evict_inode lock(&sbi->s_lock) To fix this, let's allocate bh-array with GFP_NOFS. **CVE ID: CVE-2024-42315**		
Divide By Zero	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/mglru: fix div-by-zero in	https://git.kernel.org/stable/c/8b671fe1a879923ecfb72dda6caf01460dd885ef, https://git.kernel.org/stable/c/8de7bf77f2106	O-LIN-LINU-030924/1342

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	vmpressure_calc_level() evict_folios() uses a second pass to reclaim folios that have gone through page writeback and become clean before it finishes the first pass, since folio_rotate_reclaimable() cannot handle those folios due to the isolation. The second pass tries to avoid potential double counting by deducting scan_control->nr_scanned. However, this can result in underflow of nr_scanned, under a condition where shrink_folio_list() does not increment nr_scanned, i.e., when folio_trylock() fails. The underflow can cause the divisor, i.e., scale=scanned+reclaimed in	8a5f602bb1e59adbc5ab533509d, https://git.kernel.org/stable/c/a39e38be632f0e1c908d70d1c9cd071c03faf895	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vmpressure_calc_level(), to become zero, resulting in the following crash: [exception RIP: vmpressure_work_fn+101] process_one_work at ffffffffa3313f2b Since scan_control->nr_scanned has no established semantics, the potential double counting has minimal risks. Therefore, fix the problem by not deducting scan_control->nr_scanned in evict_folios(). **CVE ID: CVE-2024-42316**		
Loop with Unreachable Exit Condition ('Infinite Loop')	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ext4: fix infinite loop when replaying fast_commit When doing fast_commit replay	https://git.kernel.org/stable/c/0619f7750f2b178a1309808832ab20d85e0ad121, https://git.kernel.org/stable/c/181e63cd595c688194e07332f9944b3a63193de2, https://git.kernel.org/stable/c/5ed0496e383cb	O-LIN-LINU-030924/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	an infinite loop may occur due to an uninitialized extent_status struct. ext4_ext_determine_insert_hole() does not detect the replay and calls ext4_es_find_extent_range(), which will return immediately without initializing the 'es' variable. Because 'es' contains garbage, an integer overflow may happen causing an infinite loop in this function, easily reproducible using fstest generic/039. This commit fixes this issue by unconditionally initializing the structure in function ext4_es_find_extent_range(). Thanks to Zhang Yi, for figuring out the real problem! **CVE ID: CVE-2024-43828**	6de120e56991385dce70bbb87c1	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Fix NULL pointer dereference in adding ancillary links In v4l2_async_create_ancillary_links(), ancillary links are created for lens and flash sub-devices. These are sub-device to sub-device links and if the async notifier is related to a V4L2 device, the source sub-device of the ancillary link is NULL, leading to a NULL pointer dereference. Check the notifier's sd field is non-NULL in v4l2_async_create_ancillary_links(). [Sakari Ailus: Reword the subject and commit messages slightly.] **CVE ID: CVE-2024-43833**	https://git.kernel.org/stable/c/249212ceb4187783af3801c57b92a5a25d410621, https://git.kernel.org/stable/c/9b4667ea67854f0b116fe22ad11ef5628c5b5b5f, https://git.kernel.org/stable/c/b87e28050d9b0959de24574d587825cfab2f13fb	O-LIN-LINU-030924/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix null pointer dereference in resolve_prog_type() for BPF_PROG_TYPE_EXT When loading a EXT program without specifying `attr->attach_prog_fd`, the `prog->aux->dst_prog` will be null. At this time, calling resolve_prog_type() anywhere will result in a null pointer dereference. Example stack trace: [8.107863] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000004 [8.108262] Mem abort info:	https://git.kernel.org/stable/c/9d40fd516aeae6779e3c84c6b96700ca76285847, https://git.kernel.org/stable/c/b29a880bb145e1f1c1df5ab88ed26b1495ff9f09, https://git.kernel.org/stable/c/f7866c35873377313ff94398f17d425b28b71de1	O-LIN-LINU-030924/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[8.108384] ESR = 0x0000000096000004 [8.108547] EC = 0x25: DABT (current EL), IL = 32 bits [8.108722] SET = 0, FnV = 0 [8.108827] EA = 0, S1PTW = 0 [8.108939] FSC = 0x04: level 0 translation fault [8.109102] Data abort info: [8.109203] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [8.109399] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [8.109614] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [8.109836] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000101354000 [8.110011] [0000000000000004] pgd=0000000000000000, p4d=0000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[8.112624] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [8.112783] Modules linked in: [8.113120] CPU: 0 PID: 99 Comm: may_access_dire Not tainted 6.10.0-rc3-next-20240613-dirty #1 [8.113230] Hardware name: linux,dummy-virt (DT) [8.113390] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [8.113429] pc : may_access_direct_pkt_data+0x24/0xa0 [8.113746] lr : add_subprog_and_kfunc+0x634/0x8e8 [8.113798] sp : ffff80008283b9f0 [8.113813] x29: ffff80008283b9f0 x28: ffff800082795048 x27: 0000000000000001 [8.113881] x26: ffff0000c0bb2600		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x25: 0000000000000000 x24: 0000000000000000 [8.113897] x23: ffff0000c1134000 x22: 000000000001864f x21: ffff0000c1138000 [8.113912] x20: 0000000000000001 x19: ffff0000c12b8000 x18: ffffffffffffffff [8.113929] x17: 0000000000000000 x16: 0000000000000000 x15: 0720072007200720 [8.113944] x14: 0720072007200720 x13: 0720072007200720 x12: 0720072007200720 [8.113958] x11: 0720072007200720 x10: 0000000000f9fca4 x9 : ffff80008021f4e4 [8.113991] x8 : 0101010101010101 x7 : 746f72705f6d656d x6 : 000000001e0e0f5f		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[8.114006] x5 : 000000000001864f x4 : ffff0000c12b8000 x3 : 000000000000001c [8.114020] x2 : 0000000000000002 x1 : 0000000000000000 x0 : 0000000000000000 [8.114126] Call trace: [8.114159] may_access_direct_pkt_data+0x24/0xa0 [8.114202] bpf_check+0x3bc/0x28c0 [8.114214] bpf_prog_load+0x658/0xa58 [8.114227] __sys_bpf+0xc50/0x2250 [8.114240] __arm64_sys_bpf+0x28/0x40 [8.114254] invoke_syscall.constprop.0+0x54/0xf0 [8.114273] do_el0_svc+0x4c/0xd8		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[8.114289] el0_svc+0x3c/0x140 [8.114305] el0t_64_sync_handler+0x134/0x150 [8.114331] el0t_64_sync+0x168/0x170 [8.114477] Code: 7100707f 54000081 f9401c00 f9403800 (b9400403) [8.118672] ---[end trace 0000000000000000]--- One way to fix it is by forcing `attach_prog_fd` non-empty when bpf_prog_load(). But this will lead to `libbpf_probe_bpf_prog_type` API broken which use verifier log to probe prog type and will log nothing if we reject invalid EXT prog before bpf_check(). Another way is by adding null check in resolve_prog_type().		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The issue was introduced by commit 4a9c7bbe2ed4 ("bpf: Resolve to prog->aux->dst_prog->type only for BPF_PROG_TYPE_EXT") which wanted to correct type resolution for BPF_PROG_TYPE_TRACING programs. Before that, the type resolution of BPF_PROG_TYPE_EXT prog actually follows the logic below: prog->aux->dst_prog ? prog->aux->dst_prog->type : prog->type; It implies that when EXT program is not yet attached to `dst_prog`, the prog type should be EXT itself. This code worked fine in the past. So just keep using it.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix this by returning `prog->type` for BPF_PROG_TYPE_EXT if `dst_prog` is not present in resolve_prog_type(). **CVE ID: CVE-2024-43837**		
Use After Free	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: cgroup/cpuset: Prevent UAF in proc_cpuset_show() An UAF can happen when /proc/cpuset is read as reported in [1]. This can be reproduced by the following methods: 1.add an mdelay(1000) before acquiring the cgroup_lock In the cgroup_path_ns function. 2.$cat /proc/<pid>/cpuset repeatly. 3.$mount -t cgroup -o cpuset cpuset	https://git.kernel.org/stable/c/1be59c97c83ccd67a519d8a49486b3a8a73ca28a, https://git.kernel.org/stable/c/29a8d4e02fd4840028c38ceb1536cc8f82a257d4, https://git.kernel.org/stable/c/29ac1d238b3bf126af36037df80d7ecc4822341e	O-LIN-LINU-030924/1346

<table>
<tr><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description &amp; CVE ID</th><th>Patch</th><th>NCIIPC ID</th></tr>
<tr><td></td><td></td><td></td><td>/sys/fs/cgroup/cpuset/
$umount /sys/fs/cgroup/cpuset/   repeatly.

The race that cause this bug can be shown as below:

(umount) | (cat /proc/<pid>/cpuset)
css_release | proc_cpuset_show
css_release_work_fn | css = task_get_css(tsk, cpuset_cgrp_id);
css_free_rwork_fn | cgroup_path_ns(css->cgroup, ...);
cgroup_destroy_root | mutex_lock(&cgroup_mutex);
rebind_subsystems |
cgroup_free_root |

| // cgrp was freed, UAF

|</td><td></td><td></td></tr>
</table>

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cgroup_path_ns_locked(cgrp,..); When the cpuset is initialized, the root node top_cpuset.css.cgrp will point to &cgrp_dfl_root.cgrp. In cgroup v1, the mount operation will allocate cgroup_root, and top_cpuset.css.cgrp will point to the allocated &cgroup_root.cgrp. When the umount operation is executed, top_cpuset.css.cgrp will be rebound to &cgrp_dfl_root.cgrp. The problem is that when rebinding to cgrp_dfl_root, there are cases where the cgroup_root allocated by setting up the root for cgroup v1 is cached. This could lead to a Use-After-Free (UAF) if it is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subsequently freed. The descendant cgroups of cgroup v1 can only be freed after the css is released. However, the css of the root will never be released, yet the cgroup_root should be freed when it is unmounted. This means that obtaining a reference to the css of the root does not guarantee that css.cgrp->root will not be freed. Fix this problem by using rcu_read_lock in proc_cpuset_show(). As cgroup_root is kfree_rcu after commit d23b5c577715 ("cgroup: Make operations on the cgroup root_list RCU safe"), css->cgroup won't be freed during the critical section. To call cgroup_path_ns_locked, css_set_lock is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed, so it is safe to replace task_get_css with task_css. [1] https://syzkaller.appspot.com/bug?extid=9b1ff7be974a403aa4cd **CVE ID: CVE-2024-43853**		
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: initialize integrity buffer to zero before writing it to media Metadata added by bio_integrity_prep is using plain kmalloc, which leads to random kernel memory being written media. For PI metadata this is limited to the app tag that isn't used by kernel generated metadata, but for non-PI metadata the entire	https://git.kernel.org/stable/c/23a19655fb56f241e592041156dfb1c6d04da644, https://git.kernel.org/stable/c/899ee2c3829c5ac14bfc7d3c4a5846c0b709b78f, https://git.kernel.org/stable/c/cf6b45ea7a8df0f61bded1dc4a8561ac6ad143d2	O-LIN-LINU-030924/1347

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer leaks kernel memory. Fix this by adding the __GFP_ZERO flag to allocations for writes. **CVE ID: CVE-2024-43854**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: md: fix deadlock between mddev_suspend and flush bio Deadlock occurs when mddev is being suspended while some flush bio is in progress. It is a complex issue. T1. the first flush is at the ending stage, it clears 'mddev->flush_bio' and tries to submit data, but is blocked because mddev is suspended by T4. T2. the second flush sets 'mddev-	https://git.kernel.org/stable/c/2d0738a8322bf4e5bfe693d16b3111928a9ccfbf, https://git.kernel.org/stable/c/32226070813140234b6c507084738e8e8385c5c6, https://git.kernel.org/stable/c/611d5cbc0b35a752e657a83eebadf40d814d006b	O-LIN-LINU-030924/1348

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>flush_bio', and attempts to queue md_submit_flush_data(), which is already running (T1) and won't execute again if on the same CPU as T1. T3. the third flush inc active_io and tries to flush, but is blocked because 'mddev->flush_bio' is not NULL (set by T2). T4. mddev_suspend() is called and waits for active_io dec to 0 which is inc by T3. T1 T2 T3 T4 (flush 1) (flush 2) (third 3) (suspend) md_submit_flush_data mddev->flush_bio = NULL; .		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			. md_flush_request . mddev->flush_bio = bio . queue submit_flushes . . . . md_handle_request . . active_io + 1 . . md_flush_request . . wait !mddev->flush_bio . . . . mddev_suspend . . wait !active_io . . . submit_flushes . queue_work		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	md_submit_flush_data . //md_submit_flush_data is already running (T1) . md_handle_request wait resume The root issue is non-atomic inc/dec of active_io during flush process. active_io is dec before md_submit_flush_data is queued, and inc soon after md_submit_flush_data() run. md_flush_request active_io + 1 submit_flushes active_io - 1 md_submit_flush_data md_handle_request active_io + 1 make_request active_io - 1 If active_io is dec after		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			md_handle_request() instead of within submit_flushes(), make_request() can be called directly intead of md_handle_request() in md_submit_flush_data(), and active_io will only inc and dec once in the whole flush process. Deadlock will be fixed. Additionally, the only difference between fixing the issue and before is that there is no return error handling of make_request(). But after previous patch cleaned md_write_start(), make_requst() only return error in raid5_make_request() by dm-raid, see commit 41425f96d7aa ("dm-raid456, md/raid456: fix a deadlock for dm-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			raid456 while io concurrent with reshape)". Since dm always splits data and flush operation into two separate io, io size of flush submitted by dm always is 0, make_request() will not be called in md_submit_flush_data(). To prevent future modifications from introducing issues, add WARN_ON to ensure make_request() no error is returned in this context. **CVE ID: CVE-2024-43855**		
Allocation of Resources Without Limits or Throttling	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse,	https://git.kernel.org/stable/c/1fe97f68fce1ba24bf823bfb0eb0956003473130, https://git.kernel.org/stable/c/22094f5f52e7bc16c5bf9613365049383650b02e, https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7	O-LIN-LINU-030924/1349

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list. If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ac2f-a84d81075b03 **CVE ID: CVE-2024-43856**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node value is NULL In imx_rproc_addr_init() "nph = of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE.	https://git.kernel.org/stable/c/2fa26ca8b786888673689ccc9da6094150939982, https://git.kernel.org/stable/c/4e13b7c23988c0a13fdca92e94296a3bc2ff9f21 , https://git.kernel.org/stable/c/6884fd0283e0831be153fb8d82d9eda8a55acaaa	O-LIN-LINU-030924/1350

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[Fixed title to fit within the prescribed 70-75 charcters] **CVE ID: CVE-2024-43860**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.45					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	O-LIN-LINU-030924/1351

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	[452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding handling is missing. Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv. **CVE ID: CVE-2024-42271**		
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/091268f3c27a5b6d7858a3bb2a0dbcc9cd26ddb5, https://git.kernel.org/stable/c/	O-LIN-LINU-030924/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	net/mlx5: Fix missing lock on sync reset reload On sync reset reload work, when remote host updates devlink on reload actions performed on that host, it misses taking devlink lock before calling devlink_remote_reload_actions_performed() which results in triggering lock assert like the following: WARNING: CPU: 4 PID: 1164 at net/devlink/core.c: 261 devl_assert_locked +0x3e/0x50 ... CPU: 4 PID: 1164 Comm: kworker/u96:6 Tainted: G S W 6.10.0-rc2+ #116 Hardware name: Supermicro SYS-2028TP-DECTR/X10DRT-PT, BIOS 2.0 12/18/2015	572f9caa9e7295f8c8822e4122c7ae8f1c412ff9, https://git.kernel.org/stable/c/5d07d1d40aabfd61bab21115639bd4f641db6002	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Workqueue: mlx5_fw_reset_events mlx5_sync_reset_reload_work [mlx5_core] RIP: 0010:devl_assert_locked+0x3e/0x50 ... Call Trace: <TASK> ? __warn+0xa4/0x210 ? devl_assert_locked+0x3e/0x50 ? report_bug+0x160/0x280 ? handle_bug+0x3f/0x80 ? exc_invalid_op+0x17/0x40 ? asm_exc_invalid_op+0x1a/0x20 ? devl_assert_locked+0x3e/0x50 devlink_notify+0x88/0x2b0 ? mlx5_attach_device		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+0x20c/0x230 [mlx5_core] ? __pfx_devlink_notify+0x10/0x10 ? process_one_work+0x4b6/0xbb0 process_one_work+0x4b6/0xbb0 [...] **CVE ID: CVE-2024-42268**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix potential null-ptr-deref in ip6table_nat_table_init(). ip6table_nat_table_init() accesses net->gen->ptr[ip6table_nat_net_ops.id], but the function is exposed to user space before the entry is allocated via register_pernet_subsys().	https://git.kernel.org/stable/c/419ee6274c5153b89c4393c1946faa4c3cad4f9e, https://git.kernel.org/stable/c/87dba44e9471b79b255d0736858a897332db9226, https://git.kernel.org/stable/c/91b6df6611b7edb28676c4f63f90c56c30d3e601	O-LIN-LINU-030924/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Let's call register_pernet_subsys() before xt_register_template(). **CVE ID: CVE-2024-42269**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix null-ptr-deref in iptable_nat_table_init(). We had a report that iptables-restore sometimes triggered null-ptr-deref at boot time. [0] The problem is that iptable_nat_table_init() is exposed to user space before the kernel fully initialises netns. In the small race window, a user could call iptable_nat_table_init() that accesses net_generic(net,	https://git.kernel.org/stable/c/08ed888b69a22647153fe2bec55b7cd0a46102cc, https://git.kernel.org/stable/c/5830aa863981d43560748aa93589c0695191d95d, https://git.kernel.org/stable/c/70014b73d7539fcbb6b4ff5f37368d7241d8e626	O-LIN-LINU-030924/1354

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iptable_nat_net_id), which is available only after registering iptable_nat_net_ops. Let's call register_pernet_subsys() before xt_register_template(). [0]: bpfilter: Loaded bpfilter_umh pid 11702 Started bpfilter BUG: kernel NULL pointer dereference, address: 0000000000000013 PF: supervisor write access in kernel mode PF: error_code(0x0002) - not-present page PGD 0 P4D 0 PREEMPT SMP NOPTI CPU: 2 PID: 11879 Comm: iptables-restor Not tainted 6.1.92-99.174.amzn2023.x86_64 #1		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	Hardware name: Amazon EC2 c6i.4xlarge/, BIOS 1.0 10/16/2017 RIP: 0010:iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat Code: 10 4c 89 f6 48 89 ef e8 0b 19 bb ff 41 89 c4 85 c0 75 38 41 83 c7 01 49 83 c6 28 41 83 ff 04 75 dc 48 8b 44 24 08 48 8b 0c 24 <48> 89 08 4c 89 ef e8 a2 3b a2 cf 48 83 c4 10 44 89 e0 5b 5d 41 5c RSP: 0018:ffffbef902843cd0 EFLAGS: 00010246 RAX: 0000000000000013 RBX: ffff9f4b052caa20 RCX: ffff9f4b20988d80 RDX: 0000000000000000 RSI: 0000000000000064 RDI: ffffffffc04201c0 RBP: ffff9f4b29394000 R08:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff9f4b07f77258 R09: ffff9f4b07f77240 R10: 0000000000000000 R11: ffff9f4b09635388 R12: 0000000000000000 R13: ffff9f4b1a3c6c00 R14: ffff9f4b20988e20 R15: 0000000000000004 FS: 00007f6284340000(0000) GS:ffff9f51fe280000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000013 CR3: 00000001d10a6005 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? xt_find_table_lock (net/netfilter/x_tables.c:1259) ? __die_body.cold (arch/x86/kernel/dumpstack.c:478 arch/x86/kernel/dumpstack.c:420) ? page_fault_oops (arch/x86/mm/fault.c:727) ? exc_page_fault (./arch/x86/include/asm/irqflags.h:40 ./arch/x86/include/asm/irqflags.h:75 arch/x86/mm/fault.c:1470 arch/x86/mm/fault.c:1518) ? asm_exc_page_fault		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(./arch/x86/include/asm/idtentry.h:570) ? iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat xt_find_table_lock (net/netfilter/x_tables.c:1259) xt_request_find_table_lock (net/netfilter/x_tables.c:1287) get_info (net/ipv4/netfilter/ip_tables.c:965) ? security_capable (security/security.c:809 (discriminator 13)) ? ns_capable (kernel/capability.c:376 kernel/capability.c:397) ? do_ipt_get_ctl (net/ipv4/netfilter/ip_tables.c:1656) ? bpfilter_send_req (net/bpfilter/bpfilter_kern.c:52) bpfilter nf_getsockopt (net/netfilter/nf_sockopt.c:116)		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_getsockopt (net/ipv4/ip_sockglue.c:1827) __sys_getsockopt (net/socket.c:2327) __x64_sys_getsockopt (net/socket.c:2342 net/socket.c:2339 net/socket.c:2339) do_syscall_64 (arch/x86/entry/common.c:51 arch/x86/entry/common.c:81) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) RIP: 0033:0x7f62844685ee Code: 48 8b 0d 45 28 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 37 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 0a c3 66 0f 1f 84 00 00 00 00 00 48 8b 15 09 RSP: 002b:00007ffd1f83d638 EFLAGS: 00000246 ORIG_RAX:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000037 RAX: ffffffffffffffda RBX: 00007ffd1f83d680 RCX: 00007f62844685ee RDX: 0000000000000040 RSI: 0000000000000000 RDI: 0000000000000004 RBP: 0000000000000004 R08: 00007ffd1f83d670 R09: 0000558798ffa2a0 R10: 00007ffd1f83d680 R11: 0000000000000246 R12: 00007ffd1f83e3b2 R13: 00007f6284 ---truncated--- **CVE ID: CVE-2024-42270**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.46					
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: xc2028: avoid use-after-free	https://git.kernel.org/stable/c/208deb6d8c3cb8c3acb1f41eb31cf68ea08726d5, https://git.kernel.org/stable/c/68594cec291ff9	O-LIN-LINU-030924/1355

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in load_firmware_cb() syzkaller reported use-after-free in load_firmware_cb() [1]. The reason is because the module allocated a struct tuner in tuner_probe(), and then the module initialization failed, the struct tuner was released. A worker which created during module initialization accesses this struct tuner later, it caused use-after-free. The process is as follows: task-6504 worker_thread tuner_probe <= alloc dvb_frontend [2] ... request_firmware_nowait <= create a worker ...	523b9feb3f43fd853dcddd1f60, https://git.kernel.org/stable/c/850304152d367f104d21c77cfbcc05806504218b	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tuner_remove <= free dvb_frontend ... request_firmware_work_func <= the firmware is ready load_firmware_cb <= but now the dvb_frontend has been freed To fix the issue, check the dvd_frontend in load_firmware_cb(), if it is null, report a warning and just return. [1]: == BUG: KASAN: use-after-free in load_firmware_cb+0x1310/0x17a0 Read of size 8 at addr ffff8000d7ca2308 by task kworker/2:3/6504		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call trace: load_firmware_cb+0x1310/0x17a0 request_firmware_work_func+0x128/0x220 process_one_work+0x770/0x1824 worker_thread+0x488/0xea0 kthread+0x300/0x430 ret_from_fork+0x10/0x20 Allocated by task 6504: kzalloc tuner_probe+0xb0/0x1430 i2c_device_probe+0x92c/0xaf0 really_probe+0x678/0xcd0 driver_probe_device+0x280/0x370 __device_attach_driver+0x220/0x330		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bus_for_each_drv+0x134/0x1c0 __device_attach+0x1f4/0x410 device_initial_probe+0x20/0x30 bus_probe_device+0x184/0x200 device_add+0x924/0x12c0 device_register+0x24/0x30 i2c_new_device+0x4e0/0xc44 v4l2_i2c_new_subdev_board+0xbc/0x290 v4l2_i2c_new_subdev+0xc8/0x104 em28xx_v4l2_init+0x1dd0/0x3770 Freed by task 6504: kfree+0x238/0x4e4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tuner_remove+0x144/0x1c0 i2c_device_remove+0xc8/0x290 __device_release_driver+0x314/0x5fc device_release_driver+0x30/0x44 bus_remove_device+0x244/0x490 device_del+0x350/0x900 device_unregister+0x28/0xd0 i2c_unregister_device+0x174/0x1d0 v4l2_device_unregister+0x224/0x380 em28xx_v4l2_init+0x1d90/0x3770 The buggy address belongs to the object at ffff8000d7ca2000 which belongs to the cache kmalloc-2k of size 2048		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	The buggy address is located 776 bytes inside of 2048-byte region [ffff8000d7ca2000, ffff8000d7ca2800) The buggy address belongs to the page: page:ffff7fe00035f280 count:1 mapcount:0 mapping:ffff8000c001f000 index:0x0 flags: 0x7ff800000000100(slab) raw: 07ff800000000100 ffff7fe00049d880 0000000300000003 ffff8000c001f000 raw: 0000000000000000 0000000080100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff8000d7ca2200:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2280: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff8000d7ca2300: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff8000d7ca2380: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2400: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == [2] Actually, it is allocated for struct tuner, and dvb_frontend is inside. **CVE ID: CVE-2024-43900**		
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0d8b26e10e680c01522d7cc14abe04c3265a92	O-LIN-LINU-030924/1356

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	net: bridge: mcast: wait for previous gc cycles when removing port syzbot hit a use-after-free[1] which is caused because the bridge doesn't make sure that all previous garbage has been collected when removing a port. What happens is: CPU 1 CPU 2 start gc cycle remove port acquire gc lock first wait for lock call br_multicasg_gc() directly acquire lock now but free port the port can be freed while grp timers still running Make sure all previous gc cycles have finished by using flush_work before	8f, https://git.kernel.org/stable/c/1e16828020c674b3be85f52685e8b80f9008f50f, https://git.kernel.org/stable/c/92c4ee25208d0f35dafc3213cdf355fbe449e078	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			freeing the port. [1] BUG: KASAN: slab-use-after-free in br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 Read of size 8 at addr ffff888071d6d000 by task syz.5.1232/9699 CPU: 1 PID: 9699 Comm: syz.5.1232 Not tainted 6.10.0-rc5-syzkaller-00021-g24ca36a562d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:114		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 call_timer_fn+0x1a3/0x610 kernel/time/timer.c:1792 expire_timers kernel/time/timer.c:1843 [inline] __run_timers+0x74b/0xaf0 kernel/time/timer.c:2417 __run_timer_base kernel/time/timer.c:2428 [inline] __run_timer_base kernel/time/timer.c:2421 [inline]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run_timer_base+0x111/0x190 kernel/time/timer.c:2437 **CVE ID: CVE-2024-44934**		
Divide By Zero	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time. [10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1 [10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[	https://git.kernel.org/stable/c/6d45e1c948a8b7ed6ceddb14319af69424db730c, https://git.kernel.org/stable/c/8f5ffd2af7274853ff91d6cd62541191d9fbd10d, https://git.kernel.org/stable/c/924f788c906dccaca30acab86c7124371e1d6f2c	O-LIN-LINU-030924/1357

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021 [10.017908] Workqueue: events_unbound padata_mt_helper [10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 : [10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330 [10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30 [10.018147] </TASK> Looking at the padata_mt_helper()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function, the only way a divide-by-0 panic can happen is when ps->chunk_size is 0. The way that chunk_size is initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least 1 no matter what the input parameters are. **CVE ID: CVE-2024-43889**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checker before passing variables Checks null pointer before passing variables to functions.	https://git.kernel.org/stable/c/1686675405d07f35eae7ff3d13a530034b899df2, https://git.kernel.org/stable/c/4cc2a94d96caeb3c975acdae7351c2f997c32175, https://git.kernel.org/stable/c/8092aa3ab8f7b	O-LIN-LINU-030924/1358

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This fixes 3 NULL_RETURNS issues reported by Coverity. **CVE ID: CVE-2024-43902**	737a34b71f91492c676a843043a	
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add NULL check for 'afb' before dereferencing in amdgpu_dm_plane_handle_cursor_update This commit adds a null check for the 'afb' variable in the amdgpu_dm_plane_handle_cursor_update function. Previously, 'afb' was assumed to be null, but was used later in the code without a null check. This could potentially lead to a null pointer dereference. Fixes the below: drivers/gpu/drm/amd/amdgpu/../di	https://git.kernel.org/stable/c/31a679a880102dee6e10985a7b1789af8dc328cc, https://git.kernel.org/stable/c/38e6f715b02b572f74677eb2f29d3b4bc6f1ddff, https://git.kernel.org/stable/c/94220b35aeba2b68da81deeefbb784d94eeb5c04	O-LIN-LINU-030924/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			splay/amdgpu_dm/amdgpu_dm_plane.c:1298 amdgpu_dm_plane_handle_cursor_update() error: we previously assumed 'afb' could be null (see line 1252) **CVE ID: CVE-2024-43903**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix the null pointer dereference for vega10_hwmgr Check return value and conduct null pointer handling to avoid null pointer dereference. **CVE ID: CVE-2024-43905**	https://git.kernel.org/stable/c/2e538944996d0dd497faf8ee81f8bfcd3aca7d80, https://git.kernel.org/stable/c/50151b7f1c79a09117837eb95b76c2de76841dab, https://git.kernel.org/stable/c/69a441473fec2fc2aa2cf56122d6c42c4266a239	O-LIN-LINU-030924/1360
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference in apply_state_adjust_rules	https://git.kernel.org/stable/c/0c065e50445aea2e0a1815f12e97ee49e02cbaac, https://git.kernel.org/stable/c/13937a40aae4efe64592ba48c057ac3c72f7fe82,	O-LIN-LINU-030924/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Check the pointer value to fix potential null pointer dereference **CVE ID: CVE-2024-43907**	https://git.kernel.org/stable/c/3a01bf2ca9f860fdc88c358567b8fa3033efcf30	
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer dereference to ras_manager Check ras_manager before using it **CVE ID: CVE-2024-43908**	https://git.kernel.org/stable/c/033187a70ba9743c73a810a006816e5553d1e7d4, https://git.kernel.org/stable/c/48cada0ac79e4775236d642e9ec5998a7c7fb7a4, https://git.kernel.org/stable/c/4c11d30c95576937c6c35e6f29884761f2dddb43	O-LIN-LINU-030924/1362
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference for smu7 optimize the code to avoid pass a null pointer (hwmgr->backend)	https://git.kernel.org/stable/c/09544cd95c688d3041328a4253bd7514972399bb, https://git.kernel.org/stable/c/1b8aa82b80bd947b68a8ab051d960a0c7935e22d, https://git.kernel.org/stable/c/37b9df457cbcf095963d18f17d6cb7dfa0a03fce	O-LIN-LINU-030924/1363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to function smu7_update_edc_leakage_table. **CVE ID: CVE-2024-43909**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_soc	https://git.kernel.org/stable/c/05e4a0fa248240efd99a539853e844f0f0a9e6a5 , https://git.kernel.org/stable/c/1407be30fc17eff918a98e0a990c0e988f11dc84, https://git.kernel.org/stable/c/52319d9d2f522ed939af31af70f8c3a0f0f67e6c	O-LIN-LINU-030924/1364

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	k() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint().		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated--- **CVE ID: CVE-2024-44935**		
Affected Version(s): From (including) 6.5 Up to (excluding) 6.10.3					
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix null reference error when checking end of zone This patch fixes a potentially null pointer being accessed by is_end_zone_blkaddr() that checks the last block of a zone when f2fs is mounted as a single device. **CVE ID: CVE-2024-43857**	https://git.kernel.org/stable/c/381cbe85592c78fbaeb3e770e3e9f3bfa3e67efb, https://git.kernel.org/stable/c/c82bc1ab2a8a5e73d9728e80c4c2ed87e8921a38	O-LIN-LINU-030924/1365
Affected Version(s): From (including) 6.5 Up to (excluding) 6.6.44					
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/5a5625a83eac91fdff1d5f0202ecfc45a31983c9,	O-LIN-LINU-030924/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			block: fix deadlock between sd_remove & sd_release Our test report the following hung task: [2538.459400] INFO: task "kworker/0:0":7 blocked for more than 188 seconds. [2538.459427] Call trace: [2538.459430] __switch_to+0x174/0x338 [2538.459436] __schedule+0x628/0x9c4 [2538.459442] schedule+0x7c/0xe8 [2538.459447] schedule_preempt_disabled+0x24/0x40 [2538.459453] __mutex_lock+0x3ec/0xf04 [2538.459456] __mutex_lock_slowpath+0x14/0x24 [2538.459459] mutex_lock+0x30/0xd8	https://git.kernel.org/stable/c/7e04da2dc7013af50ed3a2beb698d5168d1e594b, https://git.kernel.org/stable/c/f5418f48a93b69ed9e6a2281eee06b412f14a544	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2538.459462] del_gendisk+0xdc/0x350 [2538.459466] sd_remove+0x30/0x60 [2538.459470] device_release_driver_internal+0x1c4/0x2c4 [2538.459474] device_release_driver+0x18/0x28 [2538.459478] bus_remove_device+0x15c/0x174 [2538.459483] device_del+0x1d0/0x358 [2538.459488] __scsi_remove_device+0xa8/0x198 [2538.459493] scsi_forget_host+0x50/0x70 [2538.459497] scsi_remove_host+0x80/0x180 [2538.459502] usb_stor_disconnect+0x68/0xf4 [2538.459506] usb_unbind_interface+0xd4/0x280 [2538.459510] device_release_driver_internal+0x1c4/0x2c4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2538.459514] device_release_driver+0x18/0x28 [2538.459518] bus_remove_device+0x15c/0x174 [2538.459523] device_del+0x1d0/0x358 [2538.459528] usb_disable_device+0x84/0x194 [2538.459532] usb_disconnect+0xec/0x300 [2538.459537] hub_event+0xb80/0x1870 [2538.459541] process_scheduled_works+0x248/0x4dc [2538.459545] worker_thread+0x244/0x334 [2538.459549] kthread+0x114/0x1bc [2538.461001] INFO: task "fsck.":15415 blocked for more than 188 seconds. [2538.461014] Call trace: [2538.461016] __switch_to+0x174/0x338		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2538.461021] __schedule+0x628/0x9c4 [2538.461025] schedule+0x7c/0xe8 [2538.461030] blk_queue_enter+0xc4/0x160 [2538.461034] blk_mq_alloc_request+0x120/0x1d4 [2538.461037] scsi_execute_cmd+0x7c/0x23c [2538.461040] ioctl_internal_command+0x5c/0x164 [2538.461046] scsi_set_medium_removal+0x5c/0xb0 [2538.461051] sd_release+0x50/0x94 [2538.461054] blkdev_put+0x190/0x28c [2538.461058] blkdev_release+0x28/0x40 [2538.461063] __fput+0xf8/0x2a8 [2538.461066] __fput_sync+0x28/0x5c [2538.461070] __arm64_sys_close+0x84/0xe8		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2538.461073] invoke_syscall+0x58/0x114 [2538.461078] el0_svc_common+0xac/0xe0 [2538.461082] do_el0_svc+0x1c/0x28 [2538.461087] el0_svc+0x38/0x68 [2538.461090] el0t_64_sync_handler+0x68/0xbc [2538.461093] el0t_64_sync+0x1a8/0x1ac T1: T2: sd_remove del_gendisk __blk_mark_disk_dead blk_freeze_queue_start ++q->mq_freeze_depth bdev_release mutex_lock(&disk->open_mutex)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sd_release scsi_execute_cmd blk_queue_enter wait_event(!q->mq_freeze_depth) mutex_lock(&disk->open_mutex) SCSI does not set GD_OWNS_QUEUE, so QUEUE_FLAG_DYING is not set in this scenario. This is a classic ABBA deadlock. To fix the deadlock, make sure we don't try to acquire disk->open_mutex after freezing the queue. **CVE ID: CVE-2024-42294**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.10.3					
Improper Check for Unusual or	17-Aug-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/253405541be2f	O-LIN-LINU-030924/1367

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return non-zero value if the UDP media address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address. **CVE ID: CVE-2024-42284**	15ffebdeac2f4cf4b7e9144d12f, https://git.kernel.org/stable/c/2abe350db1aa599eeebc6892237d0bce0f1de62a, https://git.kernel.org/stable/c/5eea127675450583680c8170358bcba43227bd69	
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix a use-after-free related to destroying CM IDs iw_conn_req_handler() associates a new struct rdma_id_private (conn_id) with	https://git.kernel.org/stable/c/557d035fe88d78dd51664f4dc0e1896c04c97cf6, https://git.kernel.org/stable/c/7f25f296fc9bd0435be14e89bf657cd615a23574, https://git.kernel.org/stable/c/94ee7ff99b87435ec63211f632918dc7f44dac79	O-LIN-LINU-030924/1368

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			an existing struct iw_cm_id (cm_id) as follows:
			conn_id->cm_id.iw = cm_id;
			cm_id->context = conn_id;
			cm_id->cm_handler = cma_iw_handler;
			rdma_destroy_id() frees both the cm_id and the struct rdma_id_private. Make
			sure that cm_work_handler() does not trigger a use-after-free by only
			freeing of the struct rdma_id_private after all pending work has finished.
			CVE ID: CVE-2024-42285		

Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk	https://git.kernel.org/stable/c/166a0bddcc27de41fe13f861c8348e8e53e988c8 , https://git.kernel.org/stable/c/47b3dce100778001cd76f7e9188944b5cb27a76d,	O-LIN-LINU-030924/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for safer data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4]Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThread Tainted: G S W O 5.10.97-arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QT	https://git.kernel.org/stable/c/7789a1d6792af410aa9b39a1eb237ed24fa2170a	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hread,7]Hardware name: HUAWEI HUAWEI QingYun PGUX-W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9] dump_backtrace+0x0/0x1c0 [66.575469s] [pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic+0x1d8/0x3bc [66.575500s] [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42301		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a DPC event occurs concurrently to hot-removal of the same portion of the hierarchy: The dpc_handler() awaits readiness of the secondary bus below the Downstream Port where the DPC event occurred. To do so, it polls the config space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct pci_dev cause the kernel to oops.	https://git.kernel.org/stable/c/11a1f4bc47362700fcbde717292158873fb847ed, https://git.kernel.org/stable/c/2c111413f38ca5cf87557cab89f6d82b0e3433e7, https://git.kernel.org/stable/c/2cc8973bdc4d6c928ebe38b88090a2cdfe81f42f	O-LIN-LINU-030924/1370

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			That's because pci_bridge_wait_for_secondary_bus() neglects to hold a reference on the child device. Before v6.3, the function was only called on resume from system sleep or on runtime resume. Holding a reference wasn't necessary back then because the pciehp IRQ thread could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the resume_noirq phase. And runtime resume is always awaited before a PCI device is removed.) However starting with v6.3, pci_bridge_wait_for_secondary_bus() is also called on a DPC event. Commit 53b54ad074de ("PCI/DPC: Await readiness		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of secondary bus after reset"), which introduced that, failed to appreciate that pci_bridge_wait_for_secondary_bus() now needs to hold a reference on the child device because dpc_handler() and pciehp may indeed run concurrently. The commit was backported to v5.10+ stable kernels, so that's the oldest one affected. Add the missing reference acquisition. Abridged stack trace: BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464 Comm: irq/53-pcie-dpc 6.9.0 RIP: pci_bus_read_confi		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			g_dword+0x17/0x50
			pci_dev_wait()
			pci_bridge_wait_for_secondary_bus()
			dpc_reset_link()
			pcie_do_recovery()
			dpc_handler()
			CVE ID: CVE-2024-42302		

Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close There appears to be a possible use after free with vdec_close(). The firmware will add buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decoding can incur	https://git.kernel.org/stable/c/4c9d235630d35db762b85a4149bbb0be9d504c36, https://git.kernel.org/stable/c/66fa52edd32cdbb675f0803b3c4da10ea19b6635, https://git.kernel.org/stable/c/6a96041659e834dc0b172dda4b2df512d63920c2	O-LIN-LINU-030924/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a read after free for inst. Fix it by cancelling the work in vdec_close. **CVE ID: CVE-2024-42313**		
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix extent map use-after-free when adding pages to compressed bio At add_ra_bio_pages() we are accessing the extent map to calculate 'add_size' after we dropped our reference on the extent map, resulting in a use-after-free. Fix this by computing 'add_size' before dropping our extent map reference. **CVE ID: CVE-2024-42314**	https://git.kernel.org/stable/c/8e7860543a94784d744c7ce34b78a2e11beefa5c, https://git.kernel.org/stable/c/b7859ff398b6b656e1689daa860eb34837b4bb89, https://git.kernel.org/stable/c/c205565e0f2f439f278a4a94ee97b67ef7b56ae8	O-LIN-LINU-030924/1372
Off-by-one Error	17-Aug-2024	7.8	In the Linux kernel, the following	https://git.kernel.org/stable/c/99bf7c2eccff82	O-LIN-LINU-030924/1373

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: hwmon: (ltc2991) re-order conditions to fix off by one bug LTC2991_T_INT_CH_NR is 4. The st->temp_en[] array has LTC2991_MAX_CHANNEL (4) elements. Thus if "channel" is equal to LTC2991_T_INT_CH_NR then we have read one element beyond the end of the array. Flip the conditions around so that we check if "channel" is valid before using it as an array index. **CVE ID: CVE-2024-43852**	760fa23ce967cc67c8c219c6a6, https://git.kernel.org/stable/c/c180311c0a520692e2d0e9ca44dcd6c2ff1b41c4	
Improper Validation of Array Index	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree **CVE ID: CVE-2024-43858**	https://git.kernel.org/stable/c/538a27c8048f081a5ddd286f886eb986fbbc7f80, https://git.kernel.org/stable/c/55b732c8b09b41148eaab2fa8e31b0af47671e00,	O-LIN-LINU-030924/1374

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://git.kernel.org/stable/c/63f7fdf733add82f126ea00e2e48f6eba15ac4b9	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed when receiving ICMP packets with secmark set while an ICMP raw socket is being created. SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socket before that, causing the null pointer dereference. Drop the packet if label context is not set.	https://git.kernel.org/stable/c/0abe35bc48d4ec80424b1f4b3560c0e082cbd5c1, https://git.kernel.org/stable/c/290a6b88e8c19b6636ed1acc733d1458206f7697, https://git.kernel.org/stable/c/347dcb84a4874b5fb375092c08d8cc4069b94f81	O-LIN-LINU-030924/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BUG: kernel NULL pointer dereference, address: 0000000000000004c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1 3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 RIP: 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 89 f0 <8b>		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			77 4c 39 c6 7e 1f 48 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2 RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 000000000000000e RDX: ffffa92940003be8 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400 R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 R12: ffff8b574c642400 R13: 0000000000000001 R14: 0000000000000001 R15: 0000000000000000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FS: 00007fb092ea7640(0000) GS:ffff8b577bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40 apparmor_secmark_check+0xec/0x330		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security_sock_rcv_skb+0x35/0x50 sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0 ip_local_deliver_finish+0x76/0xa0 __netif_receive_skb_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 net_rx_action+0x2a4/0x380 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0 common_interrupt+0x86/0xa0 </IRQ> <TASK> asm_common_interrupt+0x26/0x40 RIP: 0010:apparmor_socket_post_create+0xb/0x200 Code: 08 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00 48 8b 1d 80 56 3f 02 48 RSP: 0018:ffffa92940ce7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000002 RDI: ffff8b574eaab740 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 0000000000000002 R14: ffff8b574eaab740 R15: ffffffffbd8e4748 ? __pfx_apparmor_so		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cket_post_create+0x10/0x10 security_socket_post_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys_socket+0x89/0x100 __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_after_hwframe+0x72/0xdc **CVE ID: CVE-2023-52889**		
Use of Uninitialized Resource	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: Initialize all fields	https://git.kernel.org/stable/c/1377de719652d868f5317ba8398b7e74c5f0430b, https://git.kern	O-LIN-LINU-030924/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in dumped nexthops struct nexthop_grp contains two reserved fields that are not initialized by nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity): # ip nexthop add id 1 dev lo # ip nexthop add id 101 group 1 # strace -e recvmsg ip nexthop get id 101 ... recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52 The fields are reserved and therefore not currently used. But as they are, they	el.org/stable/c/5cc4d71dda2dd4f1520f40e634a527022e48ccd8, https://git.kernel.org/stable/c/6d745cd0e9720282cd291d36b9db528aea18add2	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leak kernel memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure. **CVE ID: CVE-2024-42283**		
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: fix deadlock between sd_remove & sd_release Our test report the following hung task: [2538.459400] INFO: task "kworker/0:0":7 blocked for more than 188 seconds. [2538.459427] Call trace: [2538.459430] __switch_to+0x174/0x338 [2538.459436] __schedule+0x628/0x9c4	https://git.kernel.org/stable/c/5a5625a83eac91fdff1d5f0202ecfc45a31983c9, https://git.kernel.org/stable/c/7e04da2dc7013af50ed3a2beb698d5168d1e594b, https://git.kernel.org/stable/c/f5418f48a93b69ed9e6a2281eee06b412f14a544	O-LIN-LINU-030924/1377

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2538.459442] schedule+0x7c/0xe8 [2538.459447] schedule_preempt_disabled+0x24/0x40 [2538.459453] __mutex_lock+0x3ec/0xf04 [2538.459456] __mutex_lock_slowpath+0x14/0x24 [2538.459459] mutex_lock+0x30/0xd8 [2538.459462] del_gendisk+0xdc/0x350 [2538.459466] sd_remove+0x30/0x60 [2538.459470] device_release_driver_internal+0x1c4/0x2c4 [2538.459474] device_release_driver+0x18/0x28 [2538.459478] bus_remove_device+0x15c/0x174 [2538.459483] device_del+0x1d0/0x358 [2538.459488] __scsi_remove_device+0xa8/0x198		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2538.459493] scsi_forget_host+0x50/0x70 [2538.459497] scsi_remove_host+0x80/0x180 [2538.459502] usb_stor_disconnect+0x68/0xf4 [2538.459506] usb_unbind_interface+0xd4/0x280 [2538.459510] device_release_driver_internal+0x1c4/0x2c4 [2538.459514] device_release_driver+0x18/0x28 [2538.459518] bus_remove_device+0x15c/0x174 [2538.459523] device_del+0x1d0/0x358 [2538.459528] usb_disable_device+0x84/0x194 [2538.459532] usb_disconnect+0xec/0x300 [2538.459537] hub_event+0xb80/0x1870 [2538.459541] process_scheduled_works+0x248/0x4dc		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[2538.459545] worker_thread+0x244/0x334 [2538.459549] kthread+0x114/0x1bc [2538.461001] INFO: task "fsck.":15415 blocked for more than 188 seconds. [2538.461014] Call trace: [2538.461016] __switch_to+0x174/0x338 [2538.461021] __schedule+0x628/0x9c4 [2538.461025] schedule+0x7c/0xe8 [2538.461030] blk_queue_enter+0xc4/0x160 [2538.461034] blk_mq_alloc_request+0x120/0x1d4 [2538.461037] scsi_execute_cmd+0x7c/0x23c [2538.461040] ioctl_internal_command+0x5c/0x164 [2538.461046] scsi_set_medium_removal+0x5c/0xb0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	[2538.461051] sd_release+0x50/0x94 [2538.461054] blkdev_put+0x190/0x28c [2538.461058] blkdev_release+0x28/0x40 [2538.461063] __fput+0xf8/0x2a8 [2538.461066] __fput_sync+0x28/0x5c [2538.461070] __arm64_sys_close+0x84/0xe8 [2538.461073] invoke_syscall+0x58/0x114 [2538.461078] el0_svc_common+0xac/0xe0 [2538.461082] do_el0_svc+0x1c/0x28 [2538.461087] el0_svc+0x38/0x68 [2538.461090] el0t_64_sync_handler+0x68/0xbc [2538.461093] el0t_64_sync+0x1a8/0x1ac T1: T2: sd_remove del_gendisk		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__blk_mark_disk_dead blk_freeze_queue_start ++q->mq_freeze_depth bdev_release mutex_lock(&disk->open_mutex) sd_release scsi_execute_cmd blk_queue_enter wait_event(!q->mq_freeze_depth) mutex_lock(&disk->open_mutex) SCSI does not set GD_OWNS_QUEUE, so		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QUEUE_FLAG_DYING is not set in this scenario. This is a classic ABBA deadlock. To fix the deadlock, make sure we don't try to acquire disk->open_mutex after freezing the queue. **CVE ID: CVE-2024-42294**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes In psb_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	https://git.kernel.org/stable/c/13b5f3ee94bdbdc4b5f40582aab62977905aedee, https://git.kernel.org/stable/c/2df7aac81070987b0f052985856aa325a38debf6, https://git.kernel.org/stable/c/46d2ef272957879cbe30a884574320e7f7d78692	O-LIN-LINU-030924/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42309		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd. **CVE ID: CVE-2024-42310**	https://git.kernel.org/stable/c/08f45102c81ad8bc9f85f7a25e9f64e128edb87d, https://git.kernel.org/stable/c/2d209b2f862f6b8bff549ede541590a8d119da23, https://git.kernel.org/stable/c/977ee4fe895e1729cd36cc26916bbb10084713d6	O-LIN-LINU-030924/1379
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: exfat: fix potential deadlock on __exfat_get_dentry_set	https://git.kernel.org/stable/c/1d1970493c289e3f44b9ec847ed26a5dbdf56a62, https://git.kernel.org/stable/c/89fc548767a2155231128cb98726d6d2ea125	O-LIN-LINU-030924/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When accessing a file with more entries than ES_MAX_ENTRY_NUM, the bh-array is allocated in __exfat_get_entry_set. The problem is that the bh-array is allocated with GFP_KERNEL. It does not make sense. In the following cases, a deadlock for sbi->s_lock between the two processes may occur. CPU0 CPU1 ---- ---- kswapd balance_pgdat lock(fs_reclaim) exfat_iterate lock(&sbi->s_lock) exfat_readdir exfat_get_uniname_from_ext_entry exfat_get_dentry_set	6c9, https://git.kernel.org/stable/c/a7ac198f8dba791e3144c4da48a5a9b95773ee4b	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__exfat_get_dentry_set kmalloc_array ... lock(fs_reclaim) ... evict exfat_evict_inode lock(&sbi->s_lock) To fix this, let's allocate bh-array with GFP_NOFS. **CVE ID: CVE-2024-42315**		
Divide By Zero	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/mglru: fix div-by-zero in vmpressure_calc_level() evict_folios() uses a second pass to reclaim folios that have gone through page writeback and become clean before it finishes the first pass, since	https://git.kernel.org/stable/c/8b671fe1a879923ecfb72dda6caf01460dd885ef, https://git.kernel.org/stable/c/8de7bf77f21068a5f602bb1e59adbc5ab533509d, https://git.kernel.org/stable/c/a39e38be632f0e1c908d70d1c9cd071c03faf895	O-LIN-LINU-030924/1381

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	folio_rotate_reclaimable() cannot handle those folios due to the isolation. The second pass tries to avoid potential double counting by deducting scan_control->nr_scanned. However, this can result in underflow of nr_scanned, under a condition where shrink_folio_list() does not increment nr_scanned, i.e., when folio_trylock() fails. The underflow can cause the divisor, i.e., scale=scanned+reclaimed in vmpressure_calc_level(), to become zero, resulting in the following crash: [exception RIP: vmpressure_work_fn+101] process_one_work at ffffffffa3313f2b		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Since scan_control->nr_scanned has no established semantics, the potential double counting has minimal risks. Therefore, fix the problem by not deducting scan_control->nr_scanned in evict_folios(). **CVE ID: CVE-2024-42316**		
Loop with Unreachable Exit Condition ('Infinite Loop')	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ext4: fix infinite loop when replaying fast_commit When doing fast_commit replay an infinite loop may occur due to an uninitialized extent_status struct. ext4_ext_determine_insert_hole() does not detect the replay and calls ext4_es_find_extent_range(), which will	https://git.kernel.org/stable/c/0619f7750f2b178a1309808832ab20d85e0ad121, https://git.kernel.org/stable/c/181e63cd595c688194e07332f9944b3a63193de2, https://git.kernel.org/stable/c/5ed0496e383cb6de120e56991385dce70bbb87c1	O-LIN-LINU-030924/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			return immediately without initializing the 'es' variable. Because 'es' contains garbage, an integer overflow may happen causing an infinite loop in this function, easily reproducible using fstest generic/039. This commit fixes this issue by unconditionally initializing the structure in function ext4_es_find_extent_range(). Thanks to Zhang Yi, for figuring out the real problem! **CVE ID: CVE-2024-43828**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Fix NULL pointer dereference in adding ancillary links	https://git.kernel.org/stable/c/249212ceb4187783af3801c57b92a5a25d410621, https://git.kernel.org/stable/c/9b4667ea67854f0b116fe22ad11ef5628c5b5b5f, https://git.kern	O-LIN-LINU-030924/1383

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In v4l2_async_create_ancillary_links(), ancillary links are created for lens and flash sub-devices. These are sub-device to sub-device links and if the async notifier is related to a V4L2 device, the source sub-device of the ancillary link is NULL, leading to a NULL pointer dereference. Check the notifier's sd field is non-NULL in v4l2_async_create_ancillary_links(). [Sakari Ailus: Reword the subject and commit messages slightly.] **CVE ID: CVE-2024-43833**	el.org/stable/c/b87e28050d9b0959de24574d587825cfab2f13fb	
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix null pointer dereference in resolve_prog_type() for BPF_PROG_TYPE_EXT	https://git.kernel.org/stable/c/9d40fd516aeae6779e3c84c6b96700ca76285847, https://git.kernel.org/stable/c/b29a880bb145e1f1c1df5ab88ed26b1495ff9f09,	O-LIN-LINU-030924/1384

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	When loading a EXT program without specifying `attr->attach_prog_fd`, the `prog->aux->dst_prog` will be null. At this time, calling resolve_prog_type() anywhere will result in a null pointer dereference. Example stack trace: [8.107863] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000004 [8.108262] Mem abort info: [8.108384] ESR = 0x0000000096000004 [8.108547] EC = 0x25: DABT (current EL), IL = 32 bits [8.108722] SET = 0, FnV = 0	https://git.kernel.org/stable/c/f7866c35873377313ff94398f17d425b28b71de1	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[8.108827] EA = 0, S1PTW = 0 [8.108939] FSC = 0x04: level 0 translation fault [8.109102] Data abort info: [8.109203] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [8.109399] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [8.109614] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [8.109836] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000101354000 [8.110011] [0000000000000004] pgd=0000000000000000, p4d=0000000000000000 [8.112624] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [8.112783] Modules linked in: [8.113120] CPU: 0 PID: 99 Comm: may_access_dire Not tainted 6.10.0-		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rc3-next-20240613-dirty #1 [8.113230] Hardware name: linux,dummy-virt (DT) [8.113390] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [8.113429] pc : may_access_direct_pkt_data+0x24/0xa0 [8.113746] lr : add_subprog_and_kfunc+0x634/0x8e8 [8.113798] sp : ffff80008283b9f0 [8.113813] x29: ffff80008283b9f0 x28: ffff800082795048 x27: 0000000000000001 [8.113881] x26: ffff0000c0bb2600 x25: 0000000000000000 x24: 0000000000000000 [8.113897] x23: ffff0000c1134000 x22: 000000000001864f x21: ffff0000c1138000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[8.113912] x20: 0000000000000001 x19: ffff0000c12b8000 x18: ffffffffffffffff [8.113929] x17: 0000000000000000 x16: 0000000000000000 x15: 0720072007200720 [8.113944] x14: 0720072007200720 x13: 0720072007200720 x12: 0720072007200720 [8.113958] x11: 0720072007200720 x10: 0000000000f9fca4 x9 : ffff80008021f4e4 [8.113991] x8 : 0101010101010101 x7 : 746f72705f6d656d x6 : 000000001e0e0f5f [8.114006] x5 : 000000000001864f x4 : ffff0000c12b8000 x3 : 000000000000001c [8.114020] x2 : 0000000000000002 x1 : 000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 x0 : 0000000000000000 [8.114126] Call trace: [8.114159] may_access_direct_pkt_data+0x24/0xa0 [8.114202] bpf_check+0x3bc/0x28c0 [8.114214] bpf_prog_load+0x658/0xa58 [8.114227] __sys_bpf+0xc50/0x2250 [8.114240] __arm64_sys_bpf+0x28/0x40 [8.114254] invoke_syscall.constprop.0+0x54/0xf0 [8.114273] do_el0_svc+0x4c/0xd8 [8.114289] el0_svc+0x3c/0x140 [8.114305] el0t_64_sync_handler+0x134/0x150 [8.114331] el0t_64_sync+0x168/0x170 [8.114477] Code: 7100707f 54000081 f9401c00		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f9403800 (b9400403) [8.118672] ---[end trace 0000000000000000]--- One way to fix it is by forcing `attach_prog_fd` non-empty when bpf_prog_load(). But this will lead to `libbpf_probe_bpf_prog_type` API broken which use verifier log to probe prog type and will log nothing if we reject invalid EXT prog before bpf_check(). Another way is by adding null check in resolve_prog_type(). The issue was introduced by commit 4a9c7bbe2ed4 ("bpf: Resolve to prog->aux->dst_prog->type only for BPF_PROG_TYPE_EXT") which wanted to correct type resolution for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BPF_PROG_TYPE_TRACING programs. Before that, the type resolution of BPF_PROG_TYPE_EXT prog actually follows the logic below: prog->aux->dst_prog ? prog->aux->dst_prog->type : prog->type; It implies that when EXT program is not yet attached to `dst_prog`, the prog type should be EXT itself. This code worked fine in the past. So just keep using it. Fix this by returning `prog->type` for BPF_PROG_TYPE_EXT if `dst_prog` is not present in resolve_prog_type(). **CVE ID: CVE-2024-43837**		
Use After Free	17-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/1be59c97c83cc	O-LIN-LINU-030924/1385

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability has been resolved: cgroup/cpuset: Prevent UAF in proc_cpuset_show() An UAF can happen when /proc/cpuset is read as reported in [1]. This can be reproduced by the following methods: 1.add an mdelay(1000) before acquiring the cgroup_lock In the cgroup_path_ns function. 2.$cat /proc/<pid>/cpuset repeatly. 3.$mount -t cgroup -o cpuset cpuset /sys/fs/cgroup/cpuset/ $umount /sys/fs/cgroup/cpuset/ repeatly. The race that cause this bug can be shown as below:	d67a519d8a49486b3a8a73ca28a, https://git.kernel.org/stable/c/29a8d4e02fd4840028c38ceb1536cc8f82a257d4, https://git.kernel.org/stable/c/29ac1d238b3bf126af36037df80d7ecc4822341e	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			(umount) | (cat /proc/<pid>/cpuset)
			css_release | proc_cpuset_show
			css_release_work_fn | css = task_get_css(tsk, cpuset_cgrp_id);
			css_free_rwork_fn | cgroup_path_ns(css->cgroup, ...);
			cgroup_destroy_root | mutex_lock(&cgroup_mutex);
			rebind_subsystems |
			cgroup_free_root |
			| // cgrp was freed, UAF
			| cgroup_path_ns_locked(cgrp,..);
			
			When the cpuset is initialized, the root node top_cpuset.css.cgrp
			will point to &cgrp_dfl_root.cgrp. In cgroup v1, the		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mount operation will allocate cgroup_root, and top_cpuset.css.cgrp will point to the allocated &cgroup_root.cgrp. When the umount operation is executed, top_cpuset.css.cgrp will be rebound to &cgrp_dfl_root.cgrp. The problem is that when rebinding to cgrp_dfl_root, there are cases where the cgroup_root allocated by setting up the root for cgroup v1 is cached. This could lead to a Use-After-Free (UAF) if it is subsequently freed. The descendant cgroups of cgroup v1 can only be freed after the css is released. However, the css of the root will never be released, yet the cgroup_root should		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be freed when it is unmounted. This means that obtaining a reference to the css of the root does not guarantee that css.cgrp->root will not be freed. Fix this problem by using rcu_read_lock in proc_cpuset_show(). As cgroup_root is kfree_rcu after commit d23b5c577715 ("cgroup: Make operations on the cgroup root_list RCU safe"), css->cgroup won't be freed during the critical section. To call cgroup_path_ns_locked, css_set_lock is needed, so it is safe to replace task_get_css with task_css. [1] https://syzkaller.appspot.com/bug?extid=9b1ff7be974a403aa4cd		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43853		
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: block: initialize integrity buffer to zero before writing it to media Metadata added by bio_integrity_prep is using plain kmalloc, which leads to random kernel memory being written media. For PI metadata this is limited to the app tag that isn't used by kernel generated metadata, but for non-PI metadata the entire buffer leaks kernel memory. Fix this by adding the __GFP_ZERO flag to allocations for writes. **CVE ID: CVE-2024-43854**	https://git.kernel.org/stable/c/23a19655fb56f241e592041156dfb1c6d04da644, https://git.kernel.org/stable/c/899ee2c3829c5ac14bfc7d3c4a5846c0b709b78f, https://git.kernel.org/stable/c/cf6b45ea7a8df0f61bded1dc4a8561ac6ad143d2	O-LIN-LINU-030924/1386
NULL Pointer	17-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/2d0738a8322bf	O-LIN-LINU-030924/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference		🟨	vulnerability has been resolved: md: fix deadlock between mddev_suspend and flush bio Deadlock occurs when mddev is being suspended while some flush bio is in progress. It is a complex issue. T1. the first flush is at the ending stage, it clears 'mddev->flush_bio' and tries to submit data, but is blocked because mddev is suspended by T4. T2. the second flush sets 'mddev->flush_bio', and attempts to queue md_submit_flush_data(), which is already running (T1) and won't execute again if on the same CPU as T1. T3. the third flush inc active_io and	4e5bfe693d16b3111928a9ccfbf, https://git.kernel.org/stable/c/32226070813140234b6c507084738e8e8385c5c6, https://git.kernel.org/stable/c/611d5cbc0b35a752e657a83eebadf40d814d006b	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tries to flush, but is blocked because 'mddev->flush_bio' is not NULL (set by T2). T4. mddev_suspend() is called and waits for active_io dec to 0 which is inc by T3. T1 T2 T3 T4 (flush 1) (flush 2) (third 3) (suspend) md_submit_flush_data mddev->flush_bio = NULL; . . md_flush_request . mddev->flush_bio = bio . queue submit_flushes . . . . md_handle_request		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			. . active_io + 1 . . md_flush_request . . wait !mddev->flush_bio . . . . mddev_suspend . . wait !active_io . . . submit_flushes . queue_work md_submit_flush_data . //md_submit_flush_data is already running (T1) . md_handle_request wait resume The root issue is non-atomic inc/dec of active_io during flush process.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			active_io is dec before md_submit_flush_data is queued, and inc soon after md_submit_flush_data() run. md_flush_request active_io + 1 submit_flushes active_io - 1 md_submit_flush_data md_handle_request active_io + 1 make_request active_io - 1 If active_io is dec after md_handle_request() instead of within submit_flushes(), make_request() can be called directly intead of md_handle_request() in md_submit_flush_data(), and active_io will only inc and dec once in the whole flush process. Deadlock will be		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed. Additionally, the only difference between fixing the issue and before is that there is no return error handling of make_request(). But after previous patch cleaned md_write_start(), make_requst() only return error in raid5_make_request() by dm-raid, see commit 41425f96d7aa ("dm-raid456, md/raid456: fix a deadlock for dm-raid456 while io concurrent with reshape)". Since dm always splits data and flush operation into two separate io, io size of flush submitted by dm always is 0, make_request() will not be called in md_submit_flush_data(). To prevent future modifications from introducing issues,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			add WARN_ON to ensure make_request() no error is returned in this context. **CVE ID: CVE-2024-43855**		
Allocation of Resources Without Limits or Throttling	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse, then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list.	https://git.kernel.org/stable/c/1fe97f68fce1ba24bf823bfb0eb0956003473130, https://git.kernel.org/stable/c/22094f5f52e7bc16c5bf9613365049383650b02e, https://git.kernel.org/stable/c/257193083e8f43907e99ea633820fc2b3bcd24c7	O-LIN-LINU-030924/1388

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, triggering the WARN_ON() in dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03 **CVE ID: CVE-2024-43856**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to truncate preallocated blocks in f2fs_file_open() chenyuwen reports a f2fs bug as below:	https://git.kernel.org/stable/c/298b1e4182d657c3e388adcc29477904e9600ed5, https://git.kernel.org/stable/c/3ba0ae885215b325605ff7ebf6de12ac2adf204d, https://git.kernel.org/stable/c/f44a25a8bfe0c1	O-LIN-LINU-030924/1389

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Unable to handle kernel NULL pointer dereference at virtual address 0000000000000011 fscrypt_set_bio_crypt_ctx+0x78/0x1e8 f2fs_grab_read_bio+0x78/0x208 f2fs_submit_page_read+0x44/0x154 f2fs_get_read_data_page+0x288/0x5f4 f2fs_get_lock_data_page+0x60/0x190 truncate_partial_data_page+0x108/0x4fc f2fs_do_truncate_blocks+0x344/0x5f0 f2fs_truncate_blocks+0x6c/0x134 f2fs_truncate+0xd8/0x200 f2fs_iget+0x20c/0x5ac	5d33244539696cd9119cf44d18	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_garbage_collect+0x5d0/0xf6c f2fs_gc+0x22c/0x6a4 f2fs_disable_checkpoint+0xc8/0x310 f2fs_fill_super+0x14bc/0x1764 mount_bdev+0x1b4/0x21c f2fs_mount+0x20/0x30 legacy_get_tree+0x50/0xbc vfs_get_tree+0x5c/0x1b0 do_new_mount+0x298/0x4cc path_mount+0x33c/0x5fc __arm64_sys_mount+0xcc/0x15c invoke_syscall+0x60/0x150 el0_svc_common+0xb8/0xf8		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 el0t_64_sync_handler+0x88/0xec It is because inode.i_crypt_info is not initialized during below path: - mount - f2fs_fill_super - f2fs_disable_checkpoint - f2fs_gc - f2fs_iget - f2fs_truncate So, let's relocate truncation of preallocated blocks to f2fs_file_open(), after fscrypt_file_open(). **CVE ID: CVE-2024-43859**		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory	https://git.kernel.org/stable/c/2fa26ca8b786888673689ccc9da60941509399 82, https://git.kernel.org/stable/c/4e13b7c23988c	O-LIN-LINU-030924/1390

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			region when node value is NULL In imx_rproc_addr_init() "nph = of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL which is later dereferenced. Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE. [Fixed title to fit within the prescribed 70-75 charcters] **CVE ID: CVE-2024-43860**	0a13fdca92e94296a3bc2ff9f21 , https://git.kernel.org/stable/c/6884fd0283e0831be153fb8d82d9eda8a55acaaa	
Affected Version(s): From (including) 6.7 Up to (excluding) 6.10.4					
Use After Free	17-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/01437282fd3904810603f3dc98	O-LIN-LINU-030924/1391

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path is used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and swap, otherwise there is a small window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [452744.123844] Call Trace: [452744.123845] ([<0000001e87f03	d2cac6b8b6fc84, https://git.kernel.org/stable/c/37652fbef9809411cea55ea5fa1a170e299efcd0, https://git.kernel.org/stable/c/69620522c48ce8215e5eb55ffbab8cafee8f407d	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbca>] iucv_sever_path+0xc2/0xd0 [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iucv] [452744.124345] [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput+0xba/0x268 [452744.124826] [<00000000d51b382c>]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] system_call+0xe2/0x2c8 [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel panic - not syncing: Fatal exception in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding handling is missing.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ideas for a future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the tasklet functions and thus changes to all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv. **CVE ID: CVE-2024-42271**		
Improper Locking	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix missing lock on sync reset reload On sync reset reload work, when remote host updates devlink on reload actions performed on that host, it misses taking devlink lock before	https://git.kernel.org/stable/c/091268f3c27a5b6d7858a3bb2a0dbcc9cd26ddb5, https://git.kernel.org/stable/c/572f9caa9e7295f8c8822e4122c7ae8f1c412ff9, https://git.kernel.org/stable/c/5d07d1d40aabfd61bab21115639bd4f641db6002	O-LIN-LINU-030924/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling devlink_remote_reload_actions_performed() which results in triggering lock assert like the following: WARNING: CPU: 4 PID: 1164 at net/devlink/core.c: 261 devl_assert_locked +0x3e/0x50 ... CPU: 4 PID: 1164 Comm: kworker/u96:6 Tainted: G S W 6.10.0-rc2+ #116 Hardware name: Supermicro SYS-2028TP-DECTR/X10DRT-PT, BIOS 2.0 12/18/2015 Workqueue: mlx5_fw_reset_events mlx5_sync_reset_reload_work [mlx5_core] RIP: 0010:devl_assert_locked+0x3e/0x50 ... Call Trace: <TASK>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __warn+0xa4/0x210 ? devl_assert_locked+0x3e/0x50 ? report_bug+0x160/0x280 ? handle_bug+0x3f/0x80 ? exc_invalid_op+0x17/0x40 ? asm_exc_invalid_op+0x1a/0x20 ? devl_assert_locked+0x3e/0x50 devlink_notify+0x88/0x2b0 ? mlx5_attach_device+0x20c/0x230 [mlx5_core] ? __pfx_devlink_notify+0x10/0x10 ? process_one_work+0x4b6/0xbb0 process_one_work+0x4b6/0xbb0 […]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-42268		
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix potential null-ptr-deref in ip6table_nat_table_init(). ip6table_nat_table_init() accesses net->gen->ptr[ip6table_nat_net_ops.id], but the function is exposed to user space before the entry is allocated via register_pernet_subsys(). Let's call register_pernet_subsys() before xt_register_template(). **CVE ID: CVE-2024-42269**	https://git.kernel.org/stable/c/419ee6274c5153b89c4393c1946faa4c3cad4f9e, https://git.kernel.org/stable/c/87dba44e9471b79b255d0736858a897332db9226, https://git.kernel.org/stable/c/91b6df6611b7edb28676c4f63f90c56c30d3e601	O-LIN-LINU-030924/1393
NULL Pointer Dereference	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix null-ptr-deref in	https://git.kernel.org/stable/c/08ed888b69a22647153fe2bec55b7cd0a46102cc, https://git.kern	O-LIN-LINU-030924/1394

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iptable_nat_table_init(). We had a report that iptables-restore sometimes triggered null-ptr-deref at boot time. [0] The problem is that iptable_nat_table_init() is exposed to user space before the kernel fully initialises netns. In the small race window, a user could call iptable_nat_table_init() that accesses net_generic(net, iptable_nat_net_id), which is available only after registering iptable_nat_net_ops. Let's call register_pernet_subsys() before xt_register_template(). [0]:	el.org/stable/c/5830aa863981d43560748aa93589c0695191d95d, https://git.kernel.org/stable/c/70014b73d7539fcbb6b4ff5f37368d7241d8e626	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpfilter: Loaded bpfilter_umh pid 11702 Started bpfilter BUG: kernel NULL pointer dereference, address: 0000000000000013 PF: supervisor write access in kernel mode PF: error_code(0x0002) - not-present page PGD 0 P4D 0 PREEMPT SMP NOPTI CPU: 2 PID: 11879 Comm: iptables-restor Not tainted 6.1.92-99.174.amzn2023.x86_64 #1 Hardware name: Amazon EC2 c6i.4xlarge/, BIOS 1.0 10/16/2017 RIP: 0010:iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat Code: 10 4c 89 f6 48 89 ef e8 0b 19 bb ff 41 89 c4 85 c0 75 38 41 83 c7 01 49		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			83 c6 28 41 83 ff 04 75 dc 48 8b 44 24 08 48 8b 0c 24 <48> 89 08 4c 89 ef e8 a2 3b a2 cf 48 83 c4 10 44 89 e0 5b 5d 41 5c RSP: 0018:ffffbef902843cd0 EFLAGS: 00010246 RAX: 0000000000000013 RBX: ffff9f4b052caa20 RCX: ffff9f4b20988d80 RDX: 0000000000000000 RSI: 0000000000000064 RDI: ffffffffc04201c0 RBP: ffff9f4b29394000 R08: ffff9f4b07f77258 R09: ffff9f4b07f77240 R10: 0000000000000000 R11: ffff9f4b09635388 R12: 0000000000000000 R13: ffff9f4b1a3c6c00 R14: ffff9f4b20988e20 R15:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000004 FS: 00007f6284340000(0000) GS:ffff9f51fe280000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000013 CR3: 00000001d10a6005 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259)		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? xt_find_table_lock (net/netfilter/x_tables.c:1259) ? __die_body.cold (arch/x86/kernel/dumpstack.c:478 arch/x86/kernel/dumpstack.c:420) ? page_fault_oops (arch/x86/mm/fault.c:727) ? exc_page_fault (./arch/x86/include/asm/irqflags.h:40 ./arch/x86/include/asm/irqflags.h:75 arch/x86/mm/fault.c:1470 arch/x86/mm/fault.c:1518) ? asm_exc_page_fault (./arch/x86/include/asm/idtentry.h:570) ? iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat xt_find_table_lock (net/netfilter/x_tables.c:1259)		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xt_request_find_table_lock (net/netfilter/x_tables.c:1287) get_info (net/ipv4/netfilter/ip_tables.c:965) ? security_capable (security/security.c:809 (discriminator 13)) ? ns_capable (kernel/capability.c:376 kernel/capability.c:397) ? do_ipt_get_ctl (net/ipv4/netfilter/ip_tables.c:1656) ? bpfilter_send_req (net/bpfilter/bpfilter_kern.c:52) bpfilter nf_getsockopt (net/netfilter/nf_sockopt.c:116) ip_getsockopt (net/ipv4/ip_sockglue.c:1827) __sys_getsockopt (net/socket.c:2327) __x64_sys_getsockopt (net/socket.c:2342 net/socket.c:2339 net/socket.c:2339) do_syscall_64 (arch/x86/entry/c		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ommon.c:51 arch/x86/entry/common.c:81) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) RIP: 0033:0x7f62844685ee Code: 48 8b 0d 45 28 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 37 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 0a c3 66 0f 1f 84 00 00 00 00 00 48 8b 15 09 RSP: 002b:00007ffd1f83d638 EFLAGS: 00000246 ORIG_RAX: 0000000000000037 RAX: ffffffffffffffda RBX: 00007ffd1f83d680 RCX: 00007f62844685ee RDX: 0000000000000040 RSI: 0000000000000000 RDI: 0000000000000004		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: 0000000000000004 R08: 00007ffd1f83d670 R09: 0000558798ffa2a0 R10: 00007ffd1f83d680 R11: 0000000000000246 R12: 00007ffd1f83e3b2 R13: 00007f6284 ---truncated--- **CVE ID: CVE-2024-42270**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.10.5					
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: media: xc2028: avoid use-after-free in load_firmware_cb() syzkaller reported use-after-free in load_firmware_cb() [1]. The reason is because the module allocated a struct tuner in tuner_probe(), and then the module initialization failed,	https://git.kernel.org/stable/c/208deb6d8c3cb8c3acb1f41eb31cf68ea08726d5, https://git.kernel.org/stable/c/68594cec291ff9523b9feb3f43fd853dcddd1f60, https://git.kernel.org/stable/c/850304152d367f104d21c77cfbcc05806504218b	O-LIN-LINU-030924/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the struct tuner was released. A worker which created during module initialization accesses this struct tuner later, it caused use-after-free. The process is as follows: task-6504 worker_thread tuner_probe <= alloc dvb_frontend [2] ... request_firmware_nowait <= create a worker ... tuner_remove <= free dvb_frontend ... request_firmware_work_func <= the firmware is ready load_firmware_cb <= but now the dvb_frontend has been freed		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To fix the issue, check the dvd_frontend in load_firmware_cb() , if it is null, report a warning and just return. [1]: == BUG: KASAN: use-after-free in load_firmware_cb+0x1310/0x17a0 Read of size 8 at addr ffff8000d7ca2308 by task kworker/2:3/6504 Call trace: load_firmware_cb+0x1310/0x17a0 request_firmware_work_func+0x128/0x220 process_one_work+0x770/0x1824 worker_thread+0x488/0xea0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kthread+0x300/0x430 ret_from_fork+0x10/0x20 Allocated by task 6504: kzalloc tuner_probe+0xb0/0x1430 i2c_device_probe+0x92c/0xaf0 really_probe+0x678/0xcd0 driver_probe_device+0x280/0x370 __device_attach_driver+0x220/0x330 bus_for_each_drv+0x134/0x1c0 __device_attach+0x1f4/0x410 device_initial_probe+0x20/0x30 bus_probe_device+0x184/0x200		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	device_add+0x924/0x12c0 device_register+0x24/0x30 i2c_new_device+0x4e0/0xc44 v4l2_i2c_new_subdev_board+0xbc/0x290 v4l2_i2c_new_subdev+0xc8/0x104 em28xx_v4l2_init+0x1dd0/0x3770 Freed by task 6504: kfree+0x238/0x4e4 tuner_remove+0x144/0x1c0 i2c_device_remove+0xc8/0x290 __device_release_driver+0x314/0x5fc device_release_driver+0x30/0x44		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bus_remove_device+0x244/0x490 device_del+0x350/0x900 device_unregister+0x28/0xd0 i2c_unregister_device+0x174/0x1d0 v4l2_device_unregister+0x224/0x380 em28xx_v4l2_init+0x1d90/0x3770 The buggy address belongs to the object at ffff8000d7ca2000 which belongs to the cache kmalloc-2k of size 2048 The buggy address is located 776 bytes inside of 2048-byte region [ffff8000d7ca2000, ffff8000d7ca2800) The buggy address belongs to the page: page:ffff7fe00035f280 count:1		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	mapcount:0 mapping:ffff8000c001f000 index:0x0 flags: 0x7ff800000000100(slab) raw: 07ff800000000100 ffff7fe00049d880 0000000300000003 ffff8000c001f000 raw: 0000000000000000 0000000080100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff8000d7ca2200: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2280: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff8000d7ca2300: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff8000d7ca2380: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2400: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == [2] Actually, it is allocated for struct tuner, and dvb_frontend is inside. **CVE ID: CVE-2024-43900**		
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: idpf: fix UAFs when destroying the queues The second tagged commit started sometimes (very rarely, but possible) throwing WARNs from	https://git.kernel.org/stable/c/290f1c033281c1a502a3cd1c53c3a549259c491f, https://git.kernel.org/stable/c/3cde714b0e77206ed1b5cf31f28c18ba9ae946fd	O-LIN-LINU-030924/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	net/core/page_pool.c:page_pool_disable_direct_recycling(). Turned out idpf frees interrupt vectors with embedded NAPIs *before* freeing the queues making page_pools' NAPI pointers lead to freed memory before these pools are destroyed by libeth. It's not clear whether there are other accesses to the freed vectors when destroying the queues, but anyway, we usually free queue/interrupt vectors only when the queues are destroyed and the NAPIs are guaranteed to not be referenced anywhere. Invert the allocation and freeing logic making queue/interrupt vectors		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be allocated first and freed last. Vectors don't require queues to be present, so this is safe. Additionally, this change allows to remove that useless queue->q_vector pointer cleanup, as vectors are still valid when freeing the queues (+ both are freed within one function, so it's not clear why nullify the pointers at all). **CVE ID: CVE-2024-44932**		
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: wait for previous gc cycles when removing port syzbot hit a use-after-free[1] which is caused because the bridge doesn't make sure that all previous garbage has been collected when removing a	https://git.kernel.org/stable/c/0d8b26e10e680c01522d7cc14abe04c3265a928f, https://git.kernel.org/stable/c/1e16828020c674b3be85f52685e8b80f9008f50f, https://git.kernel.org/stable/c/92c4ee25208d0f35dafc3213cdf355fbe449e078	O-LIN-LINU-030924/1397

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	port. What happens is: CPU 1 CPU 2 start gc cycle remove port acquire gc lock first wait for lock call br_multicasg_gc() directly acquire lock now but free port the port can be freed while grp timers still running Make sure all previous gc cycles have finished by using flush_work before freeing the port. [1] BUG: KASAN: slab-use-after-free in br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 Read of size 8 at addr ffff888071d6d000		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	by task syz.5.1232/9699 CPU: 1 PID: 9699 Comm: syz.5.1232 Not tainted 6.10.0-rc5-syzkaller-00021-g24ca36a562d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mm/kasan/report.c:601 br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 call_timer_fn+0x1a3/0x610 kernel/time/timer.c:1792 expire_timers kernel/time/timer.c:1843 [inline] __run_timers+0x74b/0xaf0 kernel/time/timer.c:2417 __run_timer_base kernel/time/timer.c:2428 [inline] __run_timer_base kernel/time/timer.c:2421 [inline] run_timer_base+0x111/0x190 kernel/time/timer.c:2437 **CVE ID: CVE-2024-44934**		
Divide By Zero	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/6d45e1c948a8b7ed6ceddb14319af69424db730c, https://git.kern	O-LIN-LINU-030924/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time. [10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1 [10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021 [10.017908] Workqueue: events_unbound padata_mt_helper [10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 :	el.org/stable/c/8f5ffd2af7274853ff91d6cd62541191d9fbd10d, https://git.kernel.org/stable/c/924f788c906dccaca30acab86c7124371e1d6f2c	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330 [10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30 [10.018147] </TASK> Looking at the padata_mt_helper() function, the only way a divide-by-0 panic can happen is when ps->chunk_size is 0. The way that chunk_size is initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least 1 no matter what the input parameters are. **CVE ID: CVE-2024-43889**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checker before passing variables Checks null pointer before passing variables to functions. This fixes 3 NULL_RETURNS issues reported by Coverity. **CVE ID: CVE-2024-43902**	https://git.kernel.org/stable/c/1686675405d07f35eae7ff3d13a530034b899df2, https://git.kernel.org/stable/c/4cc2a94d96caeb3c975acdae7351c2f997c32175, https://git.kernel.org/stable/c/8092aa3ab8f7b737a34b71f91492c676a843043a	O-LIN-LINU-030924/1399
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/31a679a880102dee6e10985a7b1789af8dc328cc,	O-LIN-LINU-030924/1400

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/amd/display: Add NULL check for 'afb' before dereferencing in amdgpu_dm_plane_handle_cursor_update This commit adds a null check for the 'afb' variable in the amdgpu_dm_plane_handle_cursor_update function. Previously, 'afb' was assumed to be null, but was used later in the code without a null check. This could potentially lead to a null pointer dereference. Fixes the below: drivers/gpu/drm/amd/amdgpu/../display/amdgpu_dm/amdgpu_dm_plane.c:1298 amdgpu_dm_plane_handle_cursor_update() error: we previously assumed 'afb' could be null (see line 1252) **CVE ID: CVE-2024-43903**	https://git.kernel.org/stable/c/38e6f715b02b572f74677eb2f29d3b4bc6f1ddff , https://git.kernel.org/stable/c/94220b35aeba2b68da81deeefbb784d94eeb5c04	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix the null pointer dereference for vega10_hwmgr Check return value and conduct null pointer handling to avoid null pointer dereference. **CVE ID: CVE-2024-43905**	https://git.kernel.org/stable/c/2e538944996d0dd497faf8ee81f8bfcd3aca7d80, https://git.kernel.org/stable/c/50151b7f1c79a09117837eb95b76c2de76841dab, https://git.kernel.org/stable/c/69a441473fec2fc2aa2cf56122d6c42c4266a239	O-LIN-LINU-030924/1401
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/admgpu: fix dereferencing null pointer context When user space sets an invalid ta type, the pointer context will be empty. So it need to check the pointer context before using it **CVE ID: CVE-2024-43906**	https://git.kernel.org/stable/c/030ffd4d43b433bc6671d9ec34fc12c59220b95d, https://git.kernel.org/stable/c/4fd52f7c2c11d330571c6bde06e5ea508ec25c9d, https://git.kernel.org/stable/c/641dac64178ccdb9e45c92b67120316896294d05	O-LIN-LINU-030924/1402
NULL Pointer	26-Aug-2024	5.5	In the Linux kernel, the following	https://git.kernel.org/stable/c/0c065e50445aea2e0a1815f12e	O-LIN-LINU-030924/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference in apply_state_adjust_rules Check the pointer value to fix potential null pointer dereference **CVE ID: CVE-2024-43907**	97ee49e02cbaac, https://git.kernel.org/stable/c/13937a40aae4efe64592ba48c057ac3c72f7fe82, https://git.kernel.org/stable/c/3a01bf2ca9f860fdc88c358567b8fa3033efcf30	
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer dereference to ras_manager Check ras_manager before using it **CVE ID: CVE-2024-43908**	https://git.kernel.org/stable/c/033187a70ba9743c73a810a006816e5553d1e7d4, https://git.kernel.org/stable/c/48cada0ac79e4775236d642e9ec5998a7c7fb7a4, https://git.kernel.org/stable/c/4c11d30c95576937c6c35e6f29884761f2dddb43	O-LIN-LINU-030924/1404
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer	https://git.kernel.org/stable/c/09544cd95c688d3041328a4253bd7514972399bb, https://git.kern	O-LIN-LINU-030924/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference for smu7 optimize the code to avoid pass a null pointer (hwmgr->backend) to function smu7_update_edc_leakage_table. **CVE ID: CVE-2024-43909**	el.org/stable/c/1b8aa82b80bd947b68a8ab051d960a0c7935e22d, https://git.kernel.org/stable/c/37b9df457cbcf095963d18f17d6cb7dfa0a03fce	
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and	https://git.kernel.org/stable/c/05e4a0fa248240efd99a539853e844f0f0a9e6a5, https://git.kernel.org/stable/c/1407be30fc17eff918a98e0a990c0e988f11dc84, https://git.kernel.org/stable/c/52319d9d2f522ed939af31af70f8c3a0f0f67e6c	O-LIN-LINU-030924/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			concurrently closes the first listener. The second listen() calls reuseport_add_sock() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Otherwise, such sockets form multiple identical reuseport groups, and all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint(). [0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89 f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK>		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	__sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20 net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e42		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0 R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated--- **CVE ID: CVE-2024-44935**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.10.6					
N/A	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on F2FS_INLINE_DATA flag in inode during GC syzbot reports a f2fs bug as below: ------------[cut here]------------ kernel BUG at fs/f2fs/inline.c:258 ! CPU: 1 PID: 34 Comm: kworker/u8:2 Not tainted 6.9.0-rc6-	https://git.kernel.org/stable/c/26c07775fb5dc74351d1c3a2bc3cdf609b03e49f, https://git.kernel.org/stable/c/ae00e6536a2dd54b64b39e9a39548870cf835745, https://git.kernel.org/stable/c/fc01008c92f40015aeeced94750855a7111b6929	O-LIN-LINU-030924/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syzkaller-00012-g9e4bc4bcae01 #0 RIP: 0010:f2fs_write_inline_data+0x781/0x790 fs/f2fs/inline.c:258 Call Trace: f2fs_write_single_data_page+0xb65/0x1d60 fs/f2fs/data.c:2834 f2fs_write_cache_pages fs/f2fs/data.c:3133 [inline] __f2fs_write_data_pages fs/f2fs/data.c:3288 [inline] f2fs_write_data_pages+0x1efe/0x3a90 fs/f2fs/data.c:3315 do_writepages+0x35b/0x870 mm/page-writeback.c:2612 __writeback_single_inode+0x165/0x10b0 fs/fs-writeback.c:1650 writeback_sb_inodes+0x905/0x1260		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	fs/fs-writeback.c:1941 wb_writeback+0x457/0xce0 fs/fs-writeback.c:2117 wb_do_writeback fs/fs-writeback.c:2264 [inline] wb_workfn+0x410/0x1090 fs/fs-writeback.c:2304 process_one_work kernel/workqueue.c:3254 [inline] process_scheduled_works+0xa12/0x17c0 kernel/workqueue.c:3335 worker_thread+0x86d/0xd70 kernel/workqueue.c:3416 kthread+0x2f2/0x390 kernel/kthread.c:388 ret_from_fork+0x4d/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/x86/entry/entry_64.S:244 The root cause is: inline_data inode can be fuzzed, so that there may be valid blkaddr in its direct node, once f2fs triggers background GC to migrate the block, it will hit f2fs_bug_on() during dirty page writeback. Let's add sanity check on F2FS_INLINE_DATA flag in inode during GC, so that, it can forbid migrating inline_data inode's data block for fixing. **CVE ID: CVE-2024-44942**		
Affected Version(s): From (including) 6.8 Up to (excluding) 6.10.4					
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the	https://git.kernel.org/stable/c/32df4abc44f24dbec239d43e2b26d5768c5d1a78, https://git.kernel.org/stable/c/ad5fdc48f7a63b8a98493c6675	O-LIN-LINU-030924/1408

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performance extension If fetching of userspace memory fails during the main loop, all drm sync objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from commit 484de39fa5f5b7bd0c5f2e2c5265167250ef7501) **CVE ID: CVE-2024-42262**	05fe4d3864ae21	
Missing Release of Memory after Effective Lifetime	17-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the timestamp extension If fetching of userspace memory	https://git.kernel.org/stable/c/0e50fcc20bd87584840266e8004f9064a8985b4f, https://git.kernel.org/stable/c/9b5033ee2c5af6d1135a403df32d219ab57e55f9	O-LIN-LINU-030924/1409

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails during the main loop, all drm sync objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from commit 753ce4fea62182c77e1691ab4f9022008f25b62e) **CVE ID: CVE-2024-42263**		
Affected Version(s): From (including) 6.8 Up to (excluding) 6.10.5					
Use After Free	26-Aug-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: mm: list_lru: fix UAF for memory cgroup The mem_cgroup_from_slab_obj() is supposed to be called under rcu lock or cgroup_mutex or others which could	https://git.kernel.org/stable/c/4589f77c18dd98b65f45617b6d1e95313cf6fcab , https://git.kernel.org/stable/c/5161b48712dcd08ec427c450399d4d1483e21dea	O-LIN-LINU-030924/1410

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prevent returned memcg from being freed. Fix it by adding missing rcu read lock. Found by code inspection. [songmuchun@bytedance.com: only grab rcu lock when necessary, per Vlastimil] Link: https://lkml.kernel.org/r/20240801024603.1865-1-songmuchun@bytedance.com **CVE ID: CVE-2024-43888**		
NULL Pointer Dereference	26-Aug-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: platform/x86: intel-vbtn: Protect ACPI notify handler against recursion Since commit e2ffcda16290 ("ACPI: OSL: Allow Notify () handlers to run on all CPUs") ACPI notify handlers like the intel-vbtn	https://git.kernel.org/stable/c/5c9618a3b6ea94cf7bdff7702aca8bf2d777d97b, https://git.kernel.org/stable/c/e075c3b13a0a142dcd3151b25d29a24f31b7b640	O-LIN-LINU-030924/1411

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			notify_handler() may run on multiple CPU cores racing with themselves. This race gets hit on Dell Venue 7140 tablets when undocking from the keyboard, causing the handler to try and register priv->switches_dev twice, as can be seen from the dev_info() message getting logged twice: [83.861800] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after receiving a switch event [83.861858] input: Intel Virtual Switches as /devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17 [83.861865] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving a switch event After which things go seriously wrong: [83.861872] sysfs: cannot create duplicate filename '/devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17' ... [83.861967] kobject: kobject_add_internal failed for input17 with -EEXIST, don't try to register things with the same name in the same directory. [83.877338] BUG: kernel NULL pointer dereference, address: 0000000000000018 ... Protect intel-vbtn notify_handler() from racing with itself with a mutex to fix this. **CVE ID: CVE-2024-44937**		
Vendor: Microsoft					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows					
Affected Version(s): -					
N/A	21-Aug-2024	7.8	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium) **CVE ID: CVE-2024-7977**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	O-MIC-WIND-030924/1412
Insufficient Verification of Data Authenticity	21-Aug-2024	7.8	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium) **CVE ID: CVE-2024-7979**	N/A	O-MIC-WIND-030924/1413
Insufficient Verification of Data Authenticity	21-Aug-2024	7.8	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation	N/A	O-MIC-WIND-030924/1414

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted symbolic link. (Chromium security severity: Medium) **CVE ID: CVE-2024-7980**		
Use of a Broken or Risky Cryptographic Algorithm	22-Aug-2024	7.5	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID: CVE-2024-39745**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297312, https://www.ibm.com/support/pages/node/7166195	O-MIC-WIND-030924/1415
Missing Encryption of Sensitive Data	22-Aug-2024	5.9	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **CVE ID: CVE-2024-39746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/297313, https://www.ibm.com/support/pages/node/7166018	O-MIC-WIND-030924/1416

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Aug-2024	4.3	Inappropriate implementation in WebApp Installs in Google Chrome on Windows prior to 128.0.6613.84 allowed an attacker who convinced a user to install a malicious application to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID: CVE-2024-8033**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	O-MIC-WIND-030924/1417
N/A	21-Aug-2024	4.3	Inappropriate implementation in Extensions in Google Chrome on Windows prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID: CVE-2024-8035**	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html	O-MIC-WIND-030924/1418
Cross-Site Request Forgery (CSRF)	22-Aug-2024	4.3	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious	https://exchange.xforce.ibmcloud.com/vulnerabilities/297236, https://www.ibm.com/support/pages/node/7166196	O-MIC-WIND-030924/1419

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and unauthorized actions transmitted from a user that the website trusts. **CVE ID: CVE-2024-39744**		
Vendor: nepstech					
Product: ntpl-xpon1gfevn_firmware					
Affected Version(s): 1.0					
N/A	19-Aug-2024	9.8	An issue in wishnet Nepstech Wifi Router NTPL-XPON1GFEVN v1.0 allows a remote attacker to obtain sensitive information via the cookie's parameter **CVE ID: CVE-2024-42658**	N/A	O-NEP-NTPL-030924/1420
Missing Encryption of Sensitive Data	19-Aug-2024	7.5	An issue in wishnet Nepstech Wifi Router NTPL-XPON1GFEVN v1.0 allows a remote attacker to obtain sensitive information via the lack of encryption during login process **CVE ID: CVE-2024-42657**	N/A	O-NEP-NTPL-030924/1421
Vendor: nissan-global					
Product: blind_spot_protection_sensor_ecu_firmware					
Affected Version(s): -					
Use of Insufficient	19-Aug-2024	7.5	Predictable seed generation in the security access mechanism of UDS	N/A	O-NIS-BLIN-030924/1422

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			in the Blind Spot Protection Sensor ECU in Nissan Altima (2022) allows attackers to predict the requested seeds and bypass security controls via repeated ECU resets and seed requests. **CVE ID: CVE-2024-6348**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
N/A	19-Aug-2024	7.5	An issue was discovered in FRRouting (FRR) through 10.1. bgp_attr_encap in bgpd/bgp_attr.c does not check the actual remaining stream length before taking the TLV value. **CVE ID: CVE-2024-44070**	https://github.com/FRRouting/frr/pull/16497	O-RED-ENTE-030924/1423
Affected Version(s): 9.0					
N/A	19-Aug-2024	7.5	An issue was discovered in FRRouting (FRR) through 10.1. bgp_attr_encap in bgpd/bgp_attr.c does not check the actual remaining stream length	https://github.com/FRRouting/frr/pull/16497	O-RED-ENTE-030924/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before taking the TLV value. **CVE ID: CVE-2024-44070**		
Vendor: ruijie					
Product: eg2000k_firmware					
Affected Version(s): 11.1\\(6\\)b2					
Unrestricted Upload of File with Dangerous Type	26-Aug-2024	4.9	A vulnerability has been found in Ruijie EG2000K 11.1(6)B2 and classified as critical. This vulnerability affects unknown code of the file /tool/index.php?c=download&a=save. The manipulation of the argument content leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8166**	N/A	O-RUI-EG20-030924/1425
Vendor: teldat					
Product: rs123w_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-2024	4.8	Cross Site Scripting vulnerability in Teldats Router RS123, RS123w allows attacker to execute arbitrary code via the cmdcookie parameter to the upgrade/query.php page. **CVE ID: CVE-2022-39996**	N/A	O-TEL-RS12-030924/1426
Product: rs123_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Aug-2024	4.8	Cross Site Scripting vulnerability in Teldats Router RS123, RS123w allows attacker to execute arbitrary code via the cmdcookie parameter to the upgrade/query.php page. **CVE ID: CVE-2022-39996**	N/A	O-TEL-RS12-030924/1427
Vendor: tencacn					
Product: fh1206_firmware					
Affected Version(s): 1.2.0.8\\(8155\\)_en					
Out-of-bounds Write	23-Aug-2024	8.8	Tenda FH1206 V1.2.0.8(8155)_EN contains a Buffer Overflow vulnerability via the function formWrlsafeset. **CVE ID: CVE-2024-44390**	N/A	O-TEN-FH12-030924/1428

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Aug-2024	6.5	Tenda FH1206 V1.2.0.8(8155)_EN contains a Buffer Overflow vulnerability via the functino formWrlExtraGet. **CVE ID: CVE-2024-44387**	N/A	O-TEN-FH12-030924/1429
Vendor: Tenda					
Product: ax1806_firmware					
Affected Version(s): 1.0.0.1					
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo. **CVE ID: CVE-2024-44563**	N/A	O-TEN-AX18-030924/1430
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the serverName parameter in the function form_fast_setting_internet_set. **CVE ID: CVE-2024-44565**	N/A	O-TEN-AX18-030924/1431
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo.	N/A	O-TEN-AX18-030924/1432

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-44556		
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function setIptvInfo. **CVE ID: CVE-2024-44558**	N/A	O-TEN-AX18-030924/1433
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv. **CVE ID: CVE-2024-44549**	N/A	O-TEN-AX18-030924/1434
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv. **CVE ID: CVE-2024-44550**	N/A	O-TEN-AX18-030924/1435
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv. **CVE ID: CVE-2024-44551**	N/A	O-TEN-AX18-030924/1436
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via	N/A	O-TEN-AX18-030924/1437

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the adv.iptv.stballvlans parameter in the function formGetIptv. **CVE ID: CVE-2024-44552**		
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv. **CVE ID: CVE-2024-44553**	N/A	O-TEN-AX18-030924/1438
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo. **CVE ID: CVE-2024-44555**	N/A	O-TEN-AX18-030924/1439
Out-of-bounds Write	26-Aug-2024	9.8	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo. **CVE ID: CVE-2024-44557**	N/A	O-TEN-AX18-030924/1440
Product: g3_firmware					
Affected Version(s): 15.11.0.20					
Out-of-bounds Write	27-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda G3 15.11.0.20.	N/A	O-TEN-G3_F-030924/1441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected is the function formSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument sysTimePolicy 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. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8225**		
Affected Version(s): v15.11.0.20					
Out-of-bounds Write	27-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda G3 15.11.0.20. This issue affects the function formSetDebugCfg of the file /goform/setDebugCfg. The manipulation of the argument enable/level/modu	N/A	O-TEN-G3_F-030924/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			le leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8224**		
Product: o1_firmware					
Affected Version(s): 1.0.0.7\\(10648\\)					
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability has been found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early	N/A	O-TEN-O1_F-030924/1443

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8226**		
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this issue is the function fromDhcpSetSer of the file /goform/DhcpSetSer. The manipulation of the argument dhcpStartIp/dhcpEndIp/dhcpGw/dhcpMask/dhcpLeaseTime/dhcpDns1/dhcpDns2 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8227**	N/A	O-TEN-O1_F-030924/1444
Product: o5_firmware					
Affected Version(s): 1.0.0.8\\(5017\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O5 1.0.0.8(5017). It has been classified as critical. This affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8228**	N/A	O-TEN-O5_F-030924/1445
Product: o6_firmware					
Affected Version(s): 1.0.0.7\\(2054\\)					
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been declared as critical. This vulnerability affects the function frommacFilterModify of the file /goform/operateM	N/A	O-TEN-O6_F-030924/1446

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			acFilter. The manipulation of the argument mac leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8229**		
Out-of-bounds Write	28-Aug-2024	9.8	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been rated as critical. This issue affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was	N/A	O-TEN-O6_F-030924/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8230**		
Vendor: totolink					
Product: a3002r_firmware					
Affected Version(s): 1.1.1-b20200824					
Out-of-bounds Write	28-Aug-2024	9.8	TOTOLINK AC1200 Wireless Router A3002R Firmware V1.1.1-B20200824 is vulnerable to Buffer Overflow. In the boa server program's CGI handling function formWlEncrypt, there is a lack of length restriction on the wlan_ssid field. This oversight leads to potential buffer overflow under specific circumstances. For instance, by invoking the formWlanRedirect function with specific parameters to alter wlan_idx's value and subsequently invoking the formWlEncrypt function, an attacker can trigger buffer overflow, enabling arbitrary	N/A	O-TOT-A300-030924/1448

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command execution or denial of service attacks. **CVE ID: CVE-2024-34195**		
Product: ex1200l_firmware					
Affected Version(s): 9.3.5u.6146_b20201023					
Out-of-bounds Write	18-Aug-2024	9.8	A vulnerability, which was classified as critical, was found in TOTOLINK EX1200L 9.3.5u.6146_B20201023. Affected is the function setDefResponse of the file /www/cgi-bin/cstecgi.cgi. The manipulation of the argument IpAddress 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. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7908**	N/A	O-TOT-EX12-030924/1449
Out-of-bounds Write	18-Aug-2024	9.8	A vulnerability has been found in TOTOLINK	N/A	O-TOT-EX12-030924/1450

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EX1200L 9.3.5u.6146_B20201023 and classified as critical. Affected by this vulnerability is the function setLanguageCfg of the file /www/cgi-bin/cstecgi.cgi. The manipulation of the argument langType leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7909**		
Product: t10_firmware					
Affected Version(s): 4.1.8cu.5207					
Use of Hard-coded Credentials	26-Aug-2024	9.8	A vulnerability classified as critical has been found in TOTOLINK T10 AC1200 4.1.8cu.5207. Affected is an unknown function of the file /squashfs-root/web_cste/cgi-bin/product.ini of	N/A	O-TOT-T10_-030924/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component Telnet Service. The manipulation leads to hard-coded credentials. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8162**		
Product: t8_firmware					
Affected Version(s): 4.1.5cu.862_b20230228					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Aug-2024	9.8	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228 and classified as critical. Affected by this vulnerability is the function setDiagnosisCfg. The manipulation leads to os command injection. The attack can be launched remotely. NOTE: The vendor was contacted early about this disclosure but did	N/A	O-TOT-T8_F-030924/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID: CVE-2024-8075**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228 and classified as critical. Affected by this issue is the function setDiagnosisCfg. The manipulation leads to buffer overflow. The attack may be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8076**	N/A	O-TOT-T8_F-030924/1453
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been classified as critical. This affects the function setTracerouteCfg. The manipulation leads to os command injection. It is possible to initiate the attack remotely. NOTE: The vendor was contacted early	N/A	O-TOT-T8_F-030924/1454

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8077**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been declared as critical. This vulnerability affects the function setTracerouteCfg. The manipulation leads to buffer overflow. The attack can be initiated remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8078**	N/A	O-TOT-T8_F-030924/1455
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Aug-2024	9.8	A vulnerability was found in TOTOLINK AC1200 T8 4.1.5cu.862_B20230228. It has been rated as critical. This issue affects the function exportOvpn. The manipulation leads to buffer overflow. The attack may be initiated remotely. NOTE: The vendor was contacted early	N/A	O-TOT-T8_F-030924/1456

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about this disclosure but did not respond in any way. **CVE ID: CVE-2024-8079**		
Product: x6000r_firmware					
Affected Version(s): 9.4.0cu.852_b20230719					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Aug-2024	9.8	A vulnerability, which was classified as critical, has been found in TOTOLINK X6000R 9.4.0cu.852_20230719. This issue affects the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument rtLogServer leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2024-7907**	N/A	O-TOT-X600-030924/1457