National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 Apr 2024 Vol. 11 No. 7

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Codepeople					
Product: contact_form_email					
Affected Version(s): * Up to (excluding) 1.3.44					
Exposure of Sensitive Information to an Unauthorized Actor	10-Apr-2024	5.3	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in CodePeople Contact Form Email.This issue affects Contact Form Email: from n/a through 1.3.44. **CVE ID : CVE-2024-31302**	N/A	A-COD-CONT-020524/1
Vendor: Ericsson					
Product: network_manager					
Affected Version(s): * Up to (excluding) 23.1					
Improper Neutralization of Formula Elements in a CSV File	04-Apr-2024	7.1	Ericsson Network Manager (ENM), versions prior to 23.1, contains a vulnerability in the export function of application log where Improper Neutralization of Formula Elements in a CSV File can lead to code execution or information disclosure. There is limited impact to integrity and availability. The	https://www.ericsson.com/en/about-us/security/psirt/security-bulletin--ericsson-network-manager-march-2024	A-ERI-NETW-020524/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker on the adjacent network with administration access can exploit the vulnerability. **CVE ID : CVE-2024-25007**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 123.0.6312.105					
N/A	06-Apr-2024	8.8	Inappropriate implementation in V8 in Google Chrome prior to 123.0.6312.105 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-3156**	https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-020524/3
Use After Free	06-Apr-2024	8.8	Use after free in Bookmarks in Google Chrome prior to 123.0.6312.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-3158**	https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-020524/4
Improper Restriction of	06-Apr-2024	8.8	Out of bounds memory access in V8 in Google Chrome	https://chromereleases.googleblog.com/	A-GOO-CHRO-020524/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			prior to 123.0.6312.105 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-3159**	2024/04/stable-channel-update-for-desktop.html	
Vendor: IBM					
Product: websphere_application_server					
Affected Version(s): 8.5					
Use of a Broken or Risky Cryptographic Algorithm	02-Apr-2024	6.5	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security for outbound TLS connections caused by a failure to honor user configuration. IBM X-Force ID: 274812. **CVE ID : CVE-2023-50313**	https://www.ibm.com/support/pages/node/7145620	A-IBM-WEBS-020524/6
Affected Version(s): 9.0					
Use of a Broken or Risky Cryptographic Algorithm	02-Apr-2024	6.5	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security for outbound TLS connections caused by a failure to honor user configuration. IBM X-Force ID: 274812. **CVE ID : CVE-2023-50313**	https://www.ibm.com/support/pages/node/7145620	A-IBM-WEBS-020524/7
Vendor: imagely					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nextgen_gallery					
Affected Version(s): * Up to (excluding) 3.59.1					
Missing Authorization	09-Apr-2024	5.3	The WordPress Gallery Plugin – NextGEN Gallery plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_item function in versions up to, and including, 3.59. This makes it possible for unauthenticated attackers to extract sensitive data including EXIF and other metadata of any image uploaded through the plugin. **CVE ID : CVE-2024-3097**	https://plugins.trac.wordpress.org/changeset/3063940/nextgen-gallery/trunk/src/REST/Admin/Block.php?old=3003333&old_path=nextgen-gallery%2Ftrunk%2Fsrc%2FREST%2FAdmin%2FBlock.php	A-IMA-NEXT-020524/8
Vendor: ivanti					
Product: connect_secure					
Affected Version(s): 22.1					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may	N/A	A-IVA-CONN-020524/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to execution of arbitrary code **CVE ID : CVE-2024-21894**		
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-CONN-020524/10
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-CONN-020524/11
NULL Pointer	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti	N/A	A-IVA-CONN-020524/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**		
Affected Version(s): 22.2					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-CONN-020524/13
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to	N/A	A-IVA-CONN-020524/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**		
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-CONN-020524/15
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-CONN-020524/16
Affected Version(s): 22.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-CONN-020524/17
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-CONN-020524/18
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy	N/A	A-IVA-CONN-020524/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**		
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-CONN-020524/20
Affected Version(s): 22.4					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may	N/A	A-IVA-CONN-020524/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to execution of arbitrary code **CVE ID : CVE-2024-21894**		
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-CONN-020524/22
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-CONN-020524/23
NULL Pointer	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti	N/A	A-IVA-CONN-020524/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**		
Affected Version(s): 22.5					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-CONN-020524/25
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to	N/A	A-IVA-CONN-020524/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**		
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-CONN-020524/27
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-CONN-020524/28
Affected Version(s): 22.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-CONN-020524/29
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-CONN-020524/30
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy	N/A	A-IVA-CONN-020524/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**		
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-CONN-020524/32
Affected Version(s): 9.1					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may	N/A	A-IVA-CONN-020524/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to execution of arbitrary code **CVE ID : CVE-2024-21894**		
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-CONN-020524/34
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-CONN-020524/35
NULL Pointer	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti	N/A	A-IVA-CONN-020524/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**		
Product: policy_secure					
Affected Version(s): 9.0					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-POLI-020524/37
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted	N/A	A-IVA-POLI-020524/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**		
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-POLI-020524/39
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-POLI-020524/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 22.1					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-POLI-020524/41
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-POLI-020524/42
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x,	N/A	A-IVA-POLI-020524/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**		
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-POLI-020524/44
Affected Version(s): 22.2					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain	N/A	A-IVA-POLI-020524/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**		
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-POLI-020524/46
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-POLI-020524/47
NULL Pointer	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML	N/A	A-IVA-POLI-020524/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**		
Affected Version(s): 22.3					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-POLI-020524/49
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted	N/A	A-IVA-POLI-020524/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**		
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-POLI-020524/51
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-POLI-020524/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 22.4					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-POLI-020524/53
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-POLI-020524/54
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x,	N/A	A-IVA-POLI-020524/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**		
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-POLI-020524/56
Affected Version(s): 22.5					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain	N/A	A-IVA-POLI-020524/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**		
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-POLI-020524/58
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-POLI-020524/59
NULL Pointer	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML	N/A	A-IVA-POLI-020524/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**		
Affected Version(s): 22.6					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-POLI-020524/61
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted	N/A	A-IVA-POLI-020524/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**		
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**	N/A	A-IVA-POLI-020524/63
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-POLI-020524/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.1					
Out-of-bounds Write	04-Apr-2024	9.8	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack. In certain conditions this may lead to execution of arbitrary code **CVE ID : CVE-2024-21894**	N/A	A-IVA-POLI-020524/65
Out-of-bounds Write	04-Apr-2024	8.2	A heap overflow vulnerability in IPSec component of Ivanti Connect Secure (9.x 22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack or in certain conditions read contents from memory. **CVE ID : CVE-2024-22053**	N/A	A-IVA-POLI-020524/66
NULL Pointer Dereference	04-Apr-2024	7.5	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x,	N/A	A-IVA-POLI-020524/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.x) and Ivanti Policy Secure allows an unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack **CVE ID : CVE-2024-22052**		
NULL Pointer Dereference	04-Apr-2024	5.3	An XML entity expansion or XEE vulnerability in SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an unauthenticated attacker to send specially crafted XML requests in-order-to temporarily cause resource exhaustion thereby resulting in a limited-time DoS. **CVE ID : CVE-2024-22023**	N/A	A-IVA-POLI-020524/68
Vendor: layerslider					
Product: layerslider					
Affected Version(s): 7.10.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Apr-2024	7.5	The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the ls_get_popup_markup action in versions 7.9.11 and 7.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient	N/A	A-LAY-LAYE-020524/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-2879**		
Affected Version(s): 7.9.11					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Apr-2024	7.5	The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the ls_get_popup_markup action in versions 7.9.11 and 7.10.0 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-2024-2879**	N/A	A-LAY-LAYE-020524/70
Vendor: Microsoft					
Product: defender_for_iot					
Affected Version(s): * Up to (excluding) 24.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Apr-2024	8.8	Microsoft Defender for IoT Remote Code Execution Vulnerability **CVE ID : CVE-2024-29053**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29053	A-MIC-DEFE-020524/71
Affected Version(s): From (including) 22.0.0 Up to (excluding) 24.1.3					
N/A	09-Apr-2024	7.2	Microsoft Defender for IoT Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29054**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29054	A-MIC-DEFE-020524/72
N/A	09-Apr-2024	7.2	Microsoft Defender for IoT Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29055**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29055	A-MIC-DEFE-020524/73
Vendor: oceanwp					
Product: ocean_extra					
Affected Version(s): * Up to (excluding) 2.2.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Apr-2024	6.4	The Ocean Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'twitter_username' parameter in versions up to, and including, 2.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and	https://plugins.trac.wordpress.org/changeset/3066649/	A-OCE-OCEA-020524/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2024-3167**		
Vendor: Tribulant					
Product: slideshow_gallery					
Affected Version(s): * Up to (excluding) 1.7.8					
Insertion of Sensitive Information n into Log File	10-Apr-2024	5.3	Insertion of Sensitive Information into Log File vulnerability in Tribulant Slideshow Gallery.This issue affects Slideshow Gallery: from n/a through 1.7.8. **CVE ID : CVE-2024-31353**	N/A	A-TRI-SLID-020524/75
Hardware					
Vendor: Dlink					
Product: dnr-202l					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--020524/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--020524/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dnr-322l					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--020524/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--020524/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dnr-326					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--020524/80

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. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNR--020524/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-1100-4					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/83

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 immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-120					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/84

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 immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. 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--020524/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-1200-05					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. 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--020524/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-1550-04					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dns-315l					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-3272		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/91
Product: dns-320					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/93
Product: dns-320l					
Affected Version(s): -					
Use of Hard-	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which	https://supportannouncement.us.dlink.co	H-DLI-DNS--020524/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	m/security/publication.aspx?name=SAP10383	
Improper Neutralization of Special	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as	https://supportannouncement.us.dlink.com/security/p	H-DLI-DNS--020524/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	ublication.aspx?name=SAP10383	
Product: dns-320lw					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-	https://supportannouncement.us.dlink.com/security/publication.asp	H-DLI-DNS--020524/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	x?name=SAP10383	
Improper Neutralization of Special Elements used in a Command ('Comman	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-321					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-323					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-325					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-326					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-327l					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-340l					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-343					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-3273		
Product: dns-345					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dns-726-4					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-3272		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	H-DLI-DNS--020524/115
Vendor: Google					
Product: pixel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	05-Apr-2024	7.8	there is a possible way to bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2024-29748**	https://source.android.com/security/bulletin/pixel/2024-04-01	H-GOO-PIXE-020524/116
Vendor: Tenda					
Product: ax1803					
Affected Version(s): -					
Out-of-bounds Write	02-Apr-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the serviceName parameter in the function fromAdvSetMacMtuWan. **CVE ID : CVE-2024-30620**	N/A	H-TEN-AX18-020524/117
Out-of-bounds Write	02-Apr-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the serverName parameter in the function fromAdvSetMacMtuWan. **CVE ID : CVE-2024-30621**	N/A	H-TEN-AX18-020524/118
Operating System					
Vendor: Dlink					
Product: dnr-202l_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--020524/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--020524/120
Product: dnr-322l_firmware					
Affected Version(s): -					
Use of Hard-	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which	https://supportannouncement.us.dlink.co	O-DLI-DNR--020524/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	m/security/publication.aspx?name=SAP10383	
Improper Neutralization of Special	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as	https://supportannouncement.us.dlink.com/security/p	O-DLI-DNR--020524/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	ublication.aspx?name=SAP10383	
Product: dnr-326_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-	https://supportannouncement.us.dlink.com/security/publication.asp	O-DLI-DNR--020524/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	x?name=SAP10383	
Improper Neutralization of Special Elements used in a Command ('Comman	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNR--020524/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-1100-4_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-1200-05_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-120_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-1550-04_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-315l_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-320lw_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-320l_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-3273		
Product: dns-320_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dns-321_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-3272		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/142
Product: dns-323_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/144
Product: dns-325_firmware					
Affected Version(s): -					
Use of Hard-	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which	https://supportannouncement.us.dlink.co	O-DLI-DNS--020524/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	m/security/publication.aspx?name=SAP10383	
Improper Neutralization of Special	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as	https://supportannouncement.us.dlink.com/security/p	O-DLI-DNS--020524/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**	ublication.aspx?name=SAP10383	
Product: dns-326_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-	https://supportannouncement.us.dlink.com/security/publication.asp	O-DLI-DNS--020524/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**	x?name=SAP10383	
Improper Neutralization of Special Elements used in a Command ('Comman	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-327l_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-340l_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler.	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-343_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-345_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-259284. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Product: dns-726-4_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as very critical, has been found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. This issue affects some unknown processing of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument user with the input messagebus leads to hard-coded credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-259283. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3272**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-320L, DNS-325, DNS-327L and DNS-340L up to 20240403. Affected is an unknown function of the file /cgi-bin/nas_sharing.cgi of the component HTTP GET Request Handler. The manipulation of the argument system leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259284. NOTE: This vulnerability only affects products that are no longer	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383	O-DLI-DNS--020524/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-3273**		
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	05-Apr-2024	7.8	there is a possible way to bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2024-29748**	https://source.android.com/security/bulletin/pixel/2024-04-01	O-GOO-ANDR-020524/159
Use of Uninitialized Resource	05-Apr-2024	5.5	there is a possible Information Disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2024-29745**	https://source.android.com/security/bulletin/pixel/2024-04-01	O-GOO-ANDR-020524/160
Vendor: Linux					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 5.15.5					
Use After Free	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix use-after-free in lpfc_unreg_rpi() routine An error is detected with the following report when unloading the driver: "KASAN: use-after-free in lpfc_unreg_rpi+0x1b1b" The NLP_REG_LOGIN_SEND nlp_flag is set in lpfc_reg_fab_ctrl_node(), but the flag is not cleared upon completion of the login. This allows a second call to lpfc_unreg_rpi() to proceed with nlp_rpi set to LPFC_RPI_ALLOW_ERROR. This results in a use after free access when used	https://git.kernel.org/stable/c/79b20beccea3a3938a8500acef4e6b9d7c66142f, https://git.kernel.org/stable/c/dbebf865b3239595c1d4dba063b122862583b52a	O-LIN-LINU-020524/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as an rpi_ids array index. Fix by clearing the NLP_REG_LOGIN_SEND nlp_flag in lpfc_mbx_cmpl_fc_reg_login(). **CVE ID : CVE-2021-47198**		
Missing Release of Memory after Effective Lifetime	10-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: scsi: pm80xx: Fix memory leak during rmmod Driver failed to release all memory allocated. This would lead to memory leak during driver removal. Properly free memory when the module is removed. **CVE ID : CVE-2021-47193**	https://git.kernel.org/stable/c/269a4311b15f68d24e816f43f123888f241ed13d, https://git.kernel.org/stable/c/51e6ed83bb4ade7c360551fa4ae55c4eacea354b	O-LIN-LINU-020524/162
Affected Version(s): From (excluding) 5.15.0 Up to (excluding) 5.15.5					
Use After Free	10-Apr-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/37330f37f6666c7739a44b2b6b95b047ccdbed2d, https://git.ke	O-LIN-LINU-020524/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spi: fix use-after-free of the add_lock mutex Commit 6098475d4cb4 ("spi: Fix deadlock when adding SPI controllers on SPI buses") introduced a per-controller mutex. But mutex_unlock() of said lock is called after the controller is already freed: spi_unregister_controller(ctlr) -> put_device(&ctlr->dev) -> spi_controller_release(dev) -> mutex_unlock(&ctrl->add_lock) Move the put_device() after the mutex_unlock(). **CVE ID : CVE-2021-47195**	rnel.org/stable/c/6c53b45c71b4920b5e62f0ea8079a1da382b9434	
Affected Version(s): From (including) 3.6.0 Up to (excluding) 4.4.293					
Improper Initialization	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0738cdb636c21ab552eaecf905efa4	O-LIN-LINU-020524/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re-init the sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt. **CVE ID : CVE-2021-47194**	a6070e3ebc, https://git.kernel.org/stable/c/4e458abbb4a523f1413bfe15c079cf4e24c15b21, https://git.kernel.org/stable/c/52affc201fc22a1ab9a59ef0ed641a9adfcb8d13	
Affected Version(s): From (including) 4.10.0 Up to (excluding) 4.14.256					
Improper Initialization	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type	https://git.kernel.org/stable/c/0738cdb636c21ab552eaecf905efa4a6070e3ebc, https://git.kernel.org/stable/c/4e458abbb4a523f141	O-LIN-LINU-020524/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re-init the sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt. **CVE ID : CVE-2021-47194**	3bfe15c079cf4e24c15b21, https://git.kernel.org/stable/c/52affc201fc22a1ab9a59ef0ed641a9adfcb8d13	
Affected Version(s): From (including) 4.15.0 Up to (excluding) 4.19.218					
Improper Initialization	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from	https://git.kernel.org/stable/c/0738cdb636c21ab552eaecf905efa4a6070e3ebc, https://git.kernel.org/stable/c/4e458abbb4a523f1413bfe15c079cf4e24c15b21, https://git.kernel.org/stabl	O-LIN-LINU-020524/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re-init the sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt. **CVE ID : CVE-2021-47194**	e/c/52affc201fc22a1ab9a59ef0ed641a9adfcb8d13	
Affected Version(s): From (including) 4.20.0 Up to (excluding) 5.4.162					
Improper Initialization	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via	https://git.kernel.org/stable/c/0738cdb636c21ab552eaecf905efa4a6070e3ebc, https://git.kernel.org/stable/c/4e458abbb4a523f1413bfe15c079cf4e24c15b21, https://git.kernel.org/stable/c/52affc201fc22a1ab9a5	O-LIN-LINU-020524/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re-init the sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt. **CVE ID : CVE-2021-47194**	9ef0ed641a9adfcb8d13	
Affected Version(s): From (including) 4.5.0 Up to (excluding) 4.9.291					
Improper Initialization	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via send_msg(NL80211_CMD_SET_INTERFACE), it	https://git.kernel.org/stable/c/0738cdb636c21ab552eaecf905efa4a6070e3ebc, https://git.kernel.org/stable/c/4e458abbb4a523f1413bfe15c079cf4e24c15b21, https://git.kernel.org/stable/c/52affc201fc22a1ab9a59ef0ed641a9adfcb8d13	O-LIN-LINU-020524/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re-init the sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt. **CVE ID : CVE-2021-47194**		
Affected Version(s): From (including) 5.11.0 Up to (excluding) 5.15.5					
Improper Initialization	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the	https://git.kernel.org/stable/c/0738cdb636c21ab552eaecf905efa4a6070e3ebc, https://git.kernel.org/stable/c/4e458abbb4a523f1413bfe15c079cf4e24c15b21, https://git.kernel.org/stable/c/52affc201fc22a1ab9a59ef0ed641a9adfcb8d13	O-LIN-LINU-020524/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initialization of in-use data. For example, this path re-init the sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt. **CVE ID : CVE-2021-47194**		
Affected Version(s): From (including) 5.5.0 Up to (excluding) 5.10.82					
Improper Initialization	10-Apr-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_IFTYPE_ADHOC via send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re-init the	https://git.kernel.org/stable/c/0738cdb636c21ab552eaecf905efa4a6070e3ebc, https://git.kernel.org/stable/c/4e458abbb4a523f1413bfe15c079cf4e24c15b21, https://git.kernel.org/stable/c/52affc201fc22a1ab9a59ef0ed641a9adfcb8d13	O-LIN-LINU-020524/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sdata->assigned_chanctx_list while it is still an element of assigned_vifs list, and makes that linked list corrupt. **CVE ID : CVE-2021-47194**		
Vendor: Microsoft					
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20596					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/171
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/172
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.6897					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/173
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.5696					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/175
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/176
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.4291					
Improper Privilege Management	09-Apr-2024	7.8	Windows Storage Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29052	O-MIC-WIND-020524/177
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/178
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/179
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.4291					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-Apr-2024	7.8	Windows Storage Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29052	O-MIC-WIND-020524/180
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/181
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/182
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.2899					
Improper Privilege Management	09-Apr-2024	7.8	Windows Storage Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29052	O-MIC-WIND-020524/183
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/184
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/185
Product: windows_11_22h2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 10.0.22621.3447					
Improper Privilege Management	09-Apr-2024	7.8	Windows Storage Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29052	O-MIC-WIND-020524/186
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/187
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/188
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22631.3447					
Improper Privilege Management	09-Apr-2024	7.8	Windows Storage Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29052	O-MIC-WIND-020524/189
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/190
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_server_2008					
Affected Version(s): -					
Use of a Broken or Risky Cryptographic Algorithm	09-Apr-2024	4.3	Windows Authentication Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29056	O-MIC-WIND-020524/192
Product: windows_server_2012					
Affected Version(s): -					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/193
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/194
Use of a Broken or Risky Cryptographic Algorithm	09-Apr-2024	4.3	Windows Authentication Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29056	O-MIC-WIND-020524/195
Affected Version(s): r2					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/196
Time-of-check Time-of-use	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-020524/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			**CVE ID : CVE-2024-29062**	bility/CVE-2024-29062	
Use of a Broken or Risky Cryptographic Algorithm	09-Apr-2024	4.3	Windows Authentication Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29056	O-MIC-WIND-020524/198
Product: windows_server_2016					
Affected Version(s): * Up to (excluding) 10.0.14393.6897					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/199
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/200
Affected Version(s): * Up to (including) 10.0.14393.6897					
Use of a Broken or Risky Cryptographic Algorithm	09-Apr-2024	4.3	Windows Authentication Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29056	O-MIC-WIND-020524/201
Product: windows_server_2019					
Affected Version(s): * Up to (excluding) 10.0.17763.5696					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/203
Use of a Broken or Risky Cryptographic Algorithm	09-Apr-2024	4.3	Windows Authentication Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29056	O-MIC-WIND-020524/204
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348.2402					
Improper Privilege Management	09-Apr-2024	7.8	Windows Storage Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29052	O-MIC-WIND-020524/205
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/206
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/207
Use of a Broken or Risky Cryptographic Algorithm	09-Apr-2024	4.3	Windows Authentication Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29056	O-MIC-WIND-020524/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.830					
Improper Privilege Management	09-Apr-2024	7.8	Windows Storage Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29052**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29052	O-MIC-WIND-020524/209
Product: windows_server_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.830					
Out-of-bounds Write	09-Apr-2024	7.8	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29061**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29061	O-MIC-WIND-020524/210
Time-of-check Time-of-use (TOCTOU) Race Condition	09-Apr-2024	7.1	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2024-29062**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29062	O-MIC-WIND-020524/211
Use of a Broken or Risky Cryptographic Algorithm	09-Apr-2024	4.3	Windows Authentication Elevation of Privilege Vulnerability **CVE ID : CVE-2024-29056**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29056	O-MIC-WIND-020524/212
Vendor: Paloaltonetworks					
Product: pan-os					
Affected Version(s): 10.2.0					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cv	O-PAL-PAN--020524/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	e-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	
Affected Version(s): 10.2.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/215
Affected Version(s): 10.2.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**		
Affected Version(s): 10.2.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/217
Affected Version(s): 10.2.5					
Improper Neutralization of Special Elements used in a Command	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonet	O-PAL-PAN--020524/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	works.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	
Affected Version(s): 10.2.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-3400		
Affected Version(s): 10.2.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/220
Affected Version(s): 10.2.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/mo	O-PAL-PAN--020524/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	re-on-the-pan-os-cve/	
Affected Version(s): 11.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/222
Affected Version(s): 11.0.1					
Improper Neutralization of Special Elements	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature	https://security.paloaltonetworks.com/CVE-2024-3400,	O-PAL-PAN--020524/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	
Affected Version(s): 11.0.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not impacted by this vulnerability. **CVE ID : CVE-2024-3400**		
Affected Version(s): 11.0.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/225
Affected Version(s): 11.0.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.	O-PAL-PAN--020524/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	
Affected Version(s): 11.1.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/227
Affected Version(s): 11.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/228
Affected Version(s): 11.1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Apr-2024	10	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.	https://security.paloaltonetworks.com/CVE-2024-3400, https://unit42.paloaltonetworks.com/cve-2024-3400/, https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/	O-PAL-PAN--020524/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. **CVE ID : CVE-2024-3400**		
Vendor: Tenda					
Product: ax1803_firmware					
Affected Version(s): 1.0.0.1					
Out-of-bounds Write	02-Apr-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the serviceName parameter in the function fromAdvSetMacMtuWan. **CVE ID : CVE-2024-30620**	N/A	O-TEN-AX18-020524/230
Out-of-bounds Write	02-Apr-2024	9.8	Tenda AX1803 v1.0.0.1 contains a stack overflow via the serverName parameter in the function fromAdvSetMacMtuWan. **CVE ID : CVE-2024-30621**	N/A	O-TEN-AX18-020524/231