الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 22nd of April to 29th of April. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- **Critical: CVSS base score of 9.0-10.0**
- **High: CVSS base score of 7.0-8.9**
- **Medium: CVSS base score 4.0-6.9**
- **Low: CVSS base score 0.0-3.9**

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢٢ أبريل إلى ٢٩ أبريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـCVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-27524	apache - superset	Session Validation attacks in Apache Superset versions up to and including 2.0.1. Installations that have not altered the default configured SECRET_KEY according to installation instructions allow for an attacker to authenticate and access unauthorized resources. This does not affect Superset administrators who have changed the default value for SECRET_KEY config.	2023-04-24	9.8	Critical
CVE-2023-28771	zyxel - atp100_firmware	Improper error message handling in Zyxel ZyWALL/USG series firmware versions 4.60 through 4.73, VPN series firmware versions 4.60 through 5.35, USG FLEX series firmware versions 4.60 through 5.35, and ATP series firmware versions 4.60 through 5.35, which could allow an unauthenticated attacker to execute some OS commands remotely by sending crafted packets to an affected device.	2023-04-25	9.8	Critical
CVE-2023-27991	zyxel - atp200_firmware	The post-authentication command injection vulnerability in the CLI command of Zyxel ATP series firmware versions 4.32 through 5.35, USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.16 through 5.35, USG20(W)-VPN firmware versions 4.16 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow an authenticated attacker to execute some OS commands remotely.	2023-04-24	8.8	High
CVE-2023-20872	vmware - fusion	VMware Workstation and Fusion contain an out-of-bounds read/write vulnerability in SCSI CD/DVD device emulation.	2023-04-25	8.8	High
CVE-2022-41739	ibm - spectrum_scale_container_native_storage_access	IBM Spectrum Scale (IBM Spectrum Scale Container Native Storage Access 5.1.2.1 through 5.1.6.0) could allow programs running inside the container to overcome isolation mechanism and gain additional capabilities or access sensitive information on the host. IBM X-Force ID: 237815.	2023-04-26	8.4	High
CVE-2023-20869	vmware - multiple products	VMware Workstation (17.x) and VMware Fusion (13.x) contain a stack-based buffer-overflow vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine.	2023-04-25	8.2	High
CVE-2023-22913	zyxel - usg_flex_100_firmware	A post-authentication command injection vulnerability in the “account_operator.cgi” CGI program of Zyxel USG FLEX series firmware versions 4.50 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow a remote authenticated attacker to modify device configuration data, resulting in denial-of-service (DoS) conditions on an affected device.	2023-04-24	8.1	High
CVE-2023-22916	zyxel - usg_flex_100_firmware	The configuration parser of Zyxel ATP series firmware versions 5.10 through 5.35, USG FLEX series firmware versions 5.00 through 5.35, USG FLEX 50(W) firmware versions 5.10 through 5.35, USG20(W)-VPN firmware versions 5.10 through 5.35, and VPN series firmware versions 5.00 through 5.35, which fails to properly sanitize user input. A remote unauthenticated attacker could leverage the vulnerability to modify device configuration data, resulting in DoS conditions on an affected device if the attacker	2023-04-24	8.1	High

		could trick an authorized administrator to switch the management mode to the cloud mode.			
CVE-2023-2007	linux - linux_kernel	The specific flaw exists within the DPT I2O Controller driver. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the kernel.	2023-04-24	7.8	High
CVE-2023-28088	hp - multiple products	An HPE OneView appliance dump may expose SAN switch administrative credentials	2023-04-25	7.8	High
CVE-2023-20871	vmware - fusion	VMware Fusion contains a local privilege escalation vulnerability. A malicious actor with read/write access to the host operating system can elevate privileges to gain root access to the host operating system.	2023-04-25	7.8	High
CVE-2023-26286	ibm - multiple products	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX runtime services library to execute arbitrary commands. IBM X-Force ID: 248421.	2023-04-26	7.8	High
CVE-2023-2291	zohocorp - multiple products	Static credentials exist in the PostgreSQL data used in ManageEngine Access Manager Plus (AMP) build 4309, ManageEngine Password Manager Pro, and ManageEngine PAM360. These credentials could allow a malicious actor to modify configuration data that would escalate their permissions from that of a low-privileged user to an Administrative user.	2023-04-26	7.8	High
CVE-2023-31436	linux - linux_kernel	qfq_change_class in net/sched/sch_qfq.c in the Linux kernel before 6.2.13 allows an out-of-bounds write because lmax can exceed QFQ_MIN_LMAX.	2023-04-28	7.8	High
CVE-2023-28528	ibm - multiple products	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands. IBM X-Force ID: 251207.	2023-04-28	7.8	High
CVE-2023-22915	zyxel - usg_flex_100_firmware	A buffer overflow vulnerability in the “fbwifi_forward.cgi” CGI program of Zyxel USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.30 through 5.35, USG20(W)-VPN firmware versions 4.30 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow a remote unauthenticated attacker to cause DoS conditions by sending a crafted HTTP request if the Facebook WiFi function were enabled on an affected device.	2023-04-24	7.5	High
CVE-2023-22917	zyxel - usg_flex_100_firmware	A buffer overflow vulnerability in the “sdwan_iface_ipc” binary of Zyxel ATP series firmware versions 5.10 through 5.32, USG FLEX series firmware versions 5.00 through 5.32, USG FLEX 50(W) firmware versions 5.10 through 5.32, USG20(W)-VPN firmware versions 5.10 through 5.32, and VPN series firmware versions 5.00 through 5.35, which could allow a remote unauthenticated attacker to cause a core dump with a request error message on a vulnerable device by uploading a crafted configuration file.	2023-04-24	7.5	High
CVE-2023-29552	netapp - smi-s_provider	The Service Location Protocol (SLP, RFC 2608) allows an unauthenticated, remote attacker to register arbitrary services. This could allow the attacker to use spoofed UDP traffic to conduct a denial-of-service attack with a significant amplification factor.	2023-04-25	7.5	High
CVE-2023-23837	solarwinds - database_performance_analyzer	No exception handling vulnerability which revealed sensitive or excessive information to users.	2023-04-25	7.5	High
CVE-2023-0045	linux - linux_kernel	The current implementation of the prctl syscall does not issue an IBPB immediately during the syscall. The ib_prctl_set function updates the Thread Information Flags (TIFs) for the task and updates the SPEC_CTRL MSR on the function __speculation_ctrl_update, but the IBPB is only issued on the next schedule, when the TIF bits are checked. This leaves the victim vulnerable to values already injected on the BTB, prior to the prctl syscall. The patch that added the support for the conditional mitigation via prctl (ib_prctl_set) dates back to the kernel 4.9.176. We recommend upgrading past commit a664ec9158eeddd75121d39c9a0758016097fa96	2023-04-25	7.5	High
CVE-2023-27559	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may crash when using a specially crafted subquery. IBM X-Force ID: 249196.	2023-04-26	7.5	High
CVE-2023-30846	microsoft - typed-rest-client	typed-rest-client is a library for Node Rest and Http Clients with typings for use with TypeScript. Users of the typed-rest-client library version 1.7.3 or lower are vulnerable to leak authentication data to 3rd parties. The flow of the vulnerability is as follows: First, send any request with `BasicCredentialHandler`, `BearerCredentialHandler` or `PersonalAccessTokenCredentialHandler`. Second, the target host may return a redirection (3xx), with a link to a second host. Third, the next request will use the credentials to authenticate with the second host, by setting the `Authorization` header. The expected behavior is that the next request will *NOT* set the	2023-04-26	7.5	High

		`Authorization` header. The problem was fixed in version 1.8.0. There are no known workarounds.			
CVE-2023-29255	ibm - multiple products	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as it may trap when compiling a variation of an anonymous block. IBM X-Force ID: 251991.	2023-04-27	7.5	High
CVE-2023-27556	ibm - multiple products	IBM Counter Fraud Management for Safer Payments 6.1.0.00, 6.2.0.00, 6.3.0.00 through 6.3.1.03, 6.4.0.00 through 6.4.2.02 and 6.5.0.00 does not properly allocate resources without limits or throttling which could allow a remote attacker to cause a denial of service. IBM X-Force ID: 249190.	2023-04-28	7.5	High
CVE-2023-27557	ibm - multiple products	IBM Counter Fraud Management for Safer Payments 6.1.0.00 through 6.1.1.02, 6.2.0.00 through 6.2.2.02, 6.3.0.00 through 6.3.1.02, 6.4.0.00 through 6.4.2.01, and 6.5.0.00 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 249192.	2023-04-28	7.5	High
CVE-2023-22914	zyxel - usg_flex_100_firmware	A path traversal vulnerability in the “account_print.cgi” CGI program of Zyxel USG FLEX series firmware versions 4.50 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow a remote authenticated attacker with administrator privileges to execute unauthorized OS commands in the “tmp” directory by uploading a crafted file if the hotspot function were enabled.	2023-04-24	7.2	High
CVE-2022-36769	ibm - multiple products	IBM Cloud Pak for Data 4.5 and 4.6 could allow a privileged user to upload malicious files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 232034.	2023-04-26	7.2	High
CVE-2023-29257	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to remote code execution as a database administrator of one database may execute code or read/write files from another database within the same instance. IBM X-Force ID: 252011.	2023-04-26	7.2	High
CVE-2023-28089	hp - multiple products	An HPE OneView appliance dump may expose FTP credentials for c7000 Interconnect Modules	2023-04-25	7.1	High
CVE-2023-2006	linux - multiple products	A race condition was found in the Linux kernel's RxRPC network protocol, within the processing of RxRPC bundles. This issue results from the lack of proper locking when performing operations on an object. This may allow an attacker to escalate privileges and execute arbitrary code in the context of the kernel.	2023-04-24	7	High
CVE-2023-30776	apache - superset	An authenticated user with specific data permissions could access database connections stored passwords by requesting a specific REST API. This issue affects Apache Superset version 1.3.0 up to 2.0.1.	2023-04-24	6.5	Medium
CVE-2023-22918	zyxel - atp200_firmware	A post-authentication information exposure vulnerability in the CGI program of Zyxel ATP series firmware versions 4.32 through 5.35, USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.16 through 5.35, USG20(W)-VPN firmware versions 4.16 through 5.35, VPN series firmware versions 4.30 through 5.35, NWA110AX firmware version 6.50(ABTG.2) and earlier versions, WAC500 firmware version 6.50(ABVS.0) and earlier versions, and WAX510D firmware version 6.50(ABTF.2) and earlier versions, which could allow a remote authenticated attacker to retrieve encrypted information of the administrator on an affected device.	2023-04-24	6.5	Medium
CVE-2023-23838	solarwinds - database_performance_analyzer	Directory traversal and file enumeration vulnerability which allowed users to enumerate to different folders of the server.	2023-04-25	6.5	Medium
CVE-2023-23839	solarwinds - solarwinds_platform	The SolarWinds Platform was susceptible to the Exposure of Sensitive Information Vulnerability. This vulnerability allows users to access Orion.WebCommunityStrings SWIS schema object and obtain sensitive information.	2023-04-25	6.5	Medium
CVE-2023-31250	drupal - multiple products	The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.	2023-04-26	6.5	Medium
CVE-2023-30444	ibm - multiple products	IBM Watson Machine Learning on Cloud Pak for Data 4.0 and 4.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 253350.	2023-04-27	6.5	Medium
CVE-2023-2380	netgear - srx5308_firmware	A vulnerability, which was classified as problematic, was found in Netgear SRX5308 up to 4.3.5-3. Affected is an unknown function. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-227658 is the identifier assigned to this	2023-04-28	6.5	Medium

		vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
CVE-2022-25276	drupal - multiple products	The Media oEmbed iframe route does not properly validate the iframe domain setting, which allows embeds to be displayed in the context of the primary domain. Under certain circumstances, this could lead to cross-site scripting, leaked cookies, or other vulnerabilities.	2023-04-26	6.1	Medium
CVE-2023-24966	ibm - multiple products	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246904.	2023-04-27	6.1	Medium
CVE-2023-2395	netgear - srx5308_firmware	A vulnerability classified as problematic has been found in Netgear SRX5308 up to 4.3.5-3. This affects an unknown part of the component Web Management Interface. The manipulation of the argument Login.userAgent leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227673 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	6.1	Medium
CVE-2023-2396	netgear - srx5308_firmware	A vulnerability classified as problematic was found in Netgear SRX5308 up to 4.3.5-3. This vulnerability affects unknown code of the component Web Management Interface. The manipulation of the argument USERDBUsers.Password leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-227674 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	6.1	Medium
CVE-2023-20870	vmware - multiple products	VMware Workstation and Fusion contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine.	2023-04-25	6	Medium
CVE-2023-31081	linux - linux_kernel	An issue was discovered in drivers/media/test-drivers/vidtv/vidtv_bridge.c in the Linux kernel 6.2. There is a NULL pointer dereference in vidtv_mux_stop_thread. In vidtv_stop_streaming, after dvb->mux=NULL occurs, it executes vidtv_mux_stop_thread(dvb->mux).	2023-04-24	5.5	Medium
CVE-2023-31082	linux - linux_kernel	An issue was discovered in drivers/tty/n_gsm.c in the Linux kernel 6.2. There is a sleeping function called from an invalid context in gsmld_write, which will block the kernel.	2023-04-24	5.5	Medium
CVE-2023-31084	linux - linux_kernel	An issue was discovered in drivers/media/dvb-core/dvb_frontend.c in the Linux kernel 6.2. There is a blocking operation when a task is in !TASK_RUNNING. In dvb_frontend_get_event, wait_event_interruptible is called; the condition is dvb_frontend_test_event(fepriv,events). In dvb_frontend_test_event, down(&fepriv->sem) is called. However, wait_event_interruptible would put the process to sleep, and down(&fepriv->sem) may block the process.	2023-04-24	5.5	Medium
CVE-2023-31085	linux - linux_kernel	An issue was discovered in drivers/mtd/ubi/cdev.c in the Linux kernel 6.2. There is a divide-by-zero error in do_div(sz,mtd->erasesize), used indirectly by ctrl_cdev_ioctl, when mtd->erasesize is 0.	2023-04-24	5.5	Medium
CVE-2023-28086	hp - multiple products	An HPE OneView appliance dump may expose proxy credential settings	2023-04-25	5.5	Medium
CVE-2023-28087	hp - multiple products	An HPE OneView appliance dump may expose OneView user accounts	2023-04-25	5.5	Medium
CVE-2023-28090	hp - multiple products	An HPE OneView appliance dump may expose SNMPv3 read credentials	2023-04-25	5.5	Medium
CVE-2023-28084	hp - multiple products	HPE OneView and HPE OneView Global Dashboard appliance dumps may expose authentication tokens	2023-04-25	5.5	Medium
CVE-2023-2269	linux - linux_kernel	A denial of service problem was found, due to a possible recursive locking scenario, resulting in a deadlock in table_clear in drivers/md/dm-ioctl.c in the Linux Kernel Device Mapper-Multipathing sub-component.	2023-04-25	5.5	Medium
CVE-2023-22665	apache - jena	There is insufficient checking of user queries in Apache Jena versions 4.7.0 and earlier, when invoking custom scripts. It allows a remote user to execute arbitrary javascript via a SPARQL query.	2023-04-25	5.4	Medium
CVE-2023-27860	ibm - multiple products	IBM Maximo Asset Management 7.6.1.2 and 7.6.1.3 could disclose sensitive information in an error message. This information could be used in further attacks against the system. IBM X-Force ID: 249207.	2023-04-27	5.3	Medium
CVE-2020-4729	ibm - multiple products	IBM Counter Fraud Management for Safer Payments 5.7.0.00 through 5.7.0.10, 6.0.0.00 through 6.0.0.07, 6.1.0.00 through 6.1.0.05, and 6.2.0.00 through 6.2.1.00 could allow an authenticated attacker under special circumstances to send multiple specially crafted API requests that could cause the application to crash. IBM X-Force ID: 188052.	2023-04-28	5.3	Medium

CVE-2023-27990	zyxel - atp200_firmware	The XSS vulnerability in Zyxel ATP series firmware versions 4.32 through 5.35, USG FLEX series firmware versions 4.50 through 5.35, USG FLEX 50(W) firmware versions 4.16 through 5.35, USG20(W)-VPN firmware versions 4.16 through 5.35, and VPN series firmware versions 4.30 through 5.35, which could allow an authenticated attacker with administrator privileges to store malicious scripts in a vulnerable device. A successful XSS attack could then result in the stored malicious scripts being executed when the user visits the Logs page of the GUI on the device.	2023-04-24	4.8	Medium
CVE-2023-2381	netgear - srx5308_firmware	A vulnerability has been found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file scgi-bin/platform.cgi?page=bandwidth_profile.htm of the component Web Management Interface. The manipulation of the argument BandWidthProfile.ProfileName leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227659. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2382	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. Affected by this issue is some unknown functionality of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument sysLogInfo.serverName leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227660. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2383	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been classified as problematic. This affects an unknown part of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument smtpServer.fromAddr leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227661 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2384	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been declared as problematic. This vulnerability affects unknown code of the file scgi-bin/platform.cgi?page=dmz_setup.htm of the component Web Management Interface. The manipulation of the argument dhcp.SecDnsIPByte2 leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-227662 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2385	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been rated as problematic. This issue affects some unknown processing of the file scgi-bin/platform.cgi?page=ike_policies.htm of the component Web Management Interface. The manipulation of the argument IpsecIKEPolicy.IKEPolicyName leads to cross site scripting. 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-227663. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2386	netgear - srx5308_firmware	A vulnerability classified as problematic has been found in Netgear SRX5308 up to 4.3.5-3. Affected is an unknown function of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument smtpServer.toAddr leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227664. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2387	netgear - srx5308_firmware	A vulnerability classified as problematic was found in Netgear SRX5308 up to 4.3.5-3. Affected by this vulnerability is an unknown functionality of the file scgi-bin/platform.cgi?page=dmz_setup.htm of the component Web Management Interface. The manipulation of the argument winsServer1 leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227665 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2388	netgear - srx5308_firmware	A vulnerability, which was classified as problematic, has been found in Netgear SRX5308 up to 4.3.5-3. Affected by this issue is some unknown functionality of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component	2023-04-28	4.8	Medium

		Web Management Interface. The manipulation of the argument smtpServer.fromAddr leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-227666 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
CVE-2023-2389	netgear - srx5308_firmware	A vulnerability, which was classified as problematic, was found in Netgear SRX5308 up to 4.3.5-3. This affects an unknown part of the file scgi-bin/platform.cgi?page=firewall_logs_email.htm of the component Web Management Interface. The manipulation of the argument smtpServer.emailServer leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227667. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2390	netgear - srx5308_firmware	A vulnerability has been found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. This vulnerability affects unknown code of the file scgi-bin/platform.cgi?page=time_zone.htm of the component Web Management Interface. The manipulation of the argument ntp.server1 leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227668. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2391	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3 and classified as problematic. This issue affects some unknown processing of the file scgi-bin/platform.cgi?page=time_zone.htm of the component Web Management Interface. The manipulation of the argument ntp.server2 leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227669 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2392	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been classified as problematic. Affected is an unknown function of the file scgi-bin/platform.cgi?page=time_zone.htm of the component Web Management Interface. The manipulation of the argument ManualDate.minutes leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-227670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2393	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file scgi-bin/platform.cgi?page=dmz_setup.htm of the component Web Management Interface. The manipulation of the argument ConfigPort.LogicalIfName leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-2394	netgear - srx5308_firmware	A vulnerability was found in Netgear SRX5308 up to 4.3.5-3. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation of the argument wanName leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-227672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-04-28	4.8	Medium
CVE-2023-31083	linux - linux_kernel	An issue was discovered in drivers/bluetooth/hci_ldisc.c in the Linux kernel 6.2. In hci_uart_tty_ioctl, there is a race condition between HCIUARTSETPROTO and HCIUARTGETPROTO. HCI_UART_PROTO_SET is set before hu->proto is set. A NULL pointer dereference may occur.	2023-04-24	4.7	Medium
CVE-2023-2019	linux - linux_kernel	A flaw was found in the Linux kernel's netdevsim device driver, within the scheduling of events. This issue results from the improper management of a reference count. This may allow an attacker to create a denial of service condition on the system.	2023-04-24	4.4	Medium

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية
الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.