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

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

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 31 مارس إلى 6 ابريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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 31th of March to 6th 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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-48426	Google	u-boot bug that allows for u-boot shell and interrupt over UART	2024-04-05	10	Critical
CVE-2024-22004	Google	Due to length check, an attacker with privilege access on a Linux Nonsecure operating system can trigger a vulnerability and leak the secure memory from the Trusted Application	2024-04-05	10	Critical
CVE-2023-46808	Ivanti	An file upload vulnerability in Ivanti ITSM before 2023.4, allows an authenticated remote user to perform file writes to the server. Successful exploitation may lead to execution of commands in the context of non-root user.	2024-03-31	9.9	Critical
CVE-2024-3272	D-Link	** 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.	2024-04-04	9.8	Critical
CVE-2024-21894	Ivanti	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	2024-04-04	9.8	Critical
CVE-2024-25029	IBM	IBM Personal Communications 14.0.6 through 15.0.1 includes a Windows service that is vulnerable to remote code execution (RCE) and local privilege escalation (LPE). The vulnerability allows any unprivileged user with network access to a target computer to run commands with full privileges in the context of NT AUTHORITY\SYSTEM. This allows for a low privileged attacker to move laterally to affected systems and to escalate their privileges. IBM X-Force ID: 281619.	2024-04-06	9	Critical
CVE-2023-41724	Ivanti	A command injection vulnerability in Ivanti Sentry prior to 9.19.0 allows unauthenticated threat actor to execute arbitrary commands on the underlying operating system of the appliance within the same physical or logical network.	2024-03-31	8.8	High
CVE-2024-28787	IBM	IBM Security Verify Access 10.0.0 through 10.0.7 and IBM Application Gateway 20.01 through 24.03 could allow a remote attacker to obtain highly sensitive private information or cause a denial of service using a specially crafted HTTP request. IBM X-Force ID: 286584.	2024-04-04	8.7	High
CVE-2024-22053	Ivanti	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	2024-04-04	8.2	High

		service thereby causing a DoS attack or in certain conditions read contents from memory.			
CVE-2024-0172	Dell	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an improper privilege management security vulnerability. An unauthenticated local attacker could potentially exploit this vulnerability, leading to privilege escalation.	2024-04-03	7.9	High
CVE-2024-29748	Google	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.	2024-04-05	7.8	High
CVE-2024-31210	WordPress	WordPress is an open publishing platform for the Web. It's possible for a file of a type other than a zip file to be submitted as a new plugin by an administrative user on the Plugins -> Add New -> Upload Plugin screen in WordPress. If FTP credentials are requested for installation (in order to move the file into place outside of the `uploads` directory) then the uploaded file remains temporary available in the Media Library despite it not being allowed. If the `DISALLOW_FILE_EDIT` constant is set to `true` on the site _and_ FTP credentials are required when uploading a new theme or plugin, then this technically allows an RCE when the user would otherwise have no means of executing arbitrary PHP code. This issue _only_ affects Administrator level users on single site installations, and Super Admin level users on Multisite installations where it's otherwise expected that the user does not have permission to upload or execute arbitrary PHP code. Lower level users are not affected. Sites where the `DISALLOW_FILE_MODS` constant is set to `true` are not affected. Sites where an administrative user either does not need to enter FTP credentials or they have access to the valid FTP credentials, are not affected. The issue was fixed in WordPress 6.4.3 on January 30, 2024 and backported to versions 6.3.3, 6.2.4, 6.1.5, 6.0.7, 5.9.9, 5.8.9, 5.7.11, 5.6.13, 5.5.14, 5.4.15, 5.3.17, 5.2.20, 5.1.18, 5.0.21, 4.9.25, 2.8.24, 4.7.28, 4.6.28, 4.5.31, 4.4.32, 4.3.33, 4.2.37, and 4.1.40. A workaround is available. If the `DISALLOW_FILE_MODS` constant is defined as `true` then it will not be possible for any user to upload a plugin and therefore this issue will not be exploitable.	2024-04-04	7.6	High
CVE-2024-22353	IBM	IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.3 is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 280400.	2024-03-31	7.5	High
CVE-2024-1179	TP-Link	TP-Link Omada ER605 DHCPv6 Client Options Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of DHCP options. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22420.	2024-04-01	7.5	High
CVE-2024-20281	Cisco	A vulnerability in the web-based management interface of Cisco Nexus Dashboard and Cisco Nexus Dashboard hosted services could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts. Note: There are internal security mechanisms in place that limit the scope of this exploit, reducing the Security Impact Rating of this vulnerability.	2024-04-03	7.5	High
CVE-2024-20348	Cisco	A vulnerability in the Out-of-Band (OOB) Plug and Play (PnP) feature of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an unauthenticated, remote attacker to read arbitrary files. This vulnerability is due to an unauthenticated provisioning web server. An attacker could exploit this vulnerability through direct web requests to the provisioning server. A successful exploit could allow the attacker to read sensitive files in the PnP container that could facilitate further attacks on the PnP infrastructure.	2024-04-03	7.5	High
CVE-2024-22052	Ivanti	A null pointer dereference vulnerability in IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an	2024-04-04	7.5	High

		unauthenticated malicious user to send specially crafted requests in-order-to crash the service thereby causing a DoS attack			
CVE-2024-27911	Lenovo	A vulnerability was reported in some Lenovo Printers that could allow an unauthenticated attacker to obtain the administrator password.	2024-04-05	7.5	High
CVE-2024-27912	Lenovo	A denial of service vulnerability was reported in some Lenovo Printers that could allow an attacker to cause the device to crash by sending crafted LPD packets.	2024-04-05	7.5	High
CVE-2024-22328	IBM	IBM Maximo Application Suite 8.10 and 8.11 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 279950.	2024-04-06	7.5	High
CVE-2024-3273	D-Link	** 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.	2024-04-04	7.3	High
CVE-2024-29949	Hikvision	There is a command injection vulnerability in some Hikvision NVRs. This could allow an authenticated user with administrative rights to execute arbitrary commands.	2024-04-02	7.2	High
CVE-2023-38729	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server)10.5, 11.1, and 11.5 is vulnerable to sensitive information disclosure when using ADMIN_CMD with IMPORT or EXPORT. IBM X-Force ID: 262259.	2024-04-03	6.8	Medium
CVE-2024-1180	TP-Link	TP-Link Omada ER605 Access Control Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Omada ER605. Authentication is required to exploit this vulnerability. The specific issue exists within the handling of the name field in the access control user interface. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22227.	2024-04-03	6.8	Medium
CVE-2024-2312	Debian	GRUB2 does not call the module fini functions on exit, leading to Debian/Ubuntu's peimage GRUB2 module leaving UEFI system table hooks after exit. This lead to a use-after-free condition, and could possibly lead to secure boot bypass.	2024-04-05	6.7	Medium
CVE-2023-25493	Lenovo	A potential vulnerability was reported in the BIOS update tool driver for some Desktop, Smart Edge, Smart Office, and ThinkStation products that could allow a local user with elevated privileges to execute arbitrary code.	2024-04-05	6.7	Medium
CVE-2023-25494	Lenovo	A potential vulnerability were reported in the BIOS of some Desktop, Smart Edge, and ThinkStation products that could allow a local attacker with elevated privileges to write to NVRAM variables.	2024-04-05	6.7	Medium
CVE-2023-5912	Lenovo	A potential memory leakage vulnerability was reported in some Lenovo Notebook products that may allow a local attacker with elevated privileges to write to NVRAM variables.	2024-04-05	6.7	Medium
CVE-2023-50959	IBM	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2,19.0.1, 19.0.2, 19.0.3,20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1,2 2.0.2, 23.0.1, and 23.0.2 may allow end users to query more documents than expected from a connected Enterprise Content Management system when configured to use a system account. IBM X-Force ID: 275938.	2024-03-31	6.5	Medium
CVE-2023-50313	IBM	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.	2024-04-02	6.5	Medium
CVE-2024-20368	Cisco	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the	2024-04-03	6.5	Medium

		interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the targeted user.			
CVE-2024-28782	IBM	IBM QRadar Suite Software 1.10.12.0 through 1.10.18.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 285698.	2024-04-03	6.3	Medium
CVE-2024-23592	Lenovo	An authentication bypass vulnerability was reported in Lenovo devices with Synaptics fingerprint readers that could allow an attacker with physical access to replay fingerprints and bypass Windows Hello authentication.	2024-04-05	6.3	Medium
CVE-2024-25030	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 281677.	2024-04-03	6.2	Medium
CVE-2024-20310	Cisco	A vulnerability in the web-based interface of Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an authenticated user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	2024-04-03	6.1	Medium
CVE-2024-20362	Cisco	A vulnerability in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-04-03	6.1	Medium
CVE-2024-20282	Cisco	A vulnerability in Cisco Nexus Dashboard could allow an authenticated, local attacker with valid rescue-user credentials to elevate privileges to root on an affected device. This vulnerability is due to insufficient protections for a sensitive access token. An attacker could exploit this vulnerability by using this token to access resources within the device infrastructure. A successful exploit could allow an attacker to gain root access to the filesystem or hosted containers on an affected device.	2024-04-03	6	Medium
CVE-2024-27268	IBM	IBM WebSphere Application Server Liberty 18.0.0.2 through 24.0.0.3 is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 284574.	2024-04-04	5.9	Medium
CVE-2024-25027	IBM	IBM Security Verify Access 10.0.6 could disclose sensitive snapshot information due to missing encryption. IBM X-Force ID: 281607.	2024-03-31	5.5	Medium
CVE-2024-20332	Cisco	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a server-side request forgery (SSRF) attack through an affected device. This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected device. To successfully exploit this vulnerability, the attacker would need valid Super Admin credentials.	2024-04-03	5.5	Medium
CVE-2024-20334	Cisco	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) could allow a low-privileged, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-04-03	5.5	Medium

CVE-2024-31211	WordPress	WordPress is an open publishing platform for the Web. Unserialization of instances of the `WP_HTML_Token` class allows for code execution via its `__destruct()` magic method. This issue was fixed in WordPress 6.4.2 on December 6th, 2023. Versions prior to 6.4.0 are not affected.	2024-04-04	5.5	Medium
CVE-2024-29745	Google	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.	2024-04-05	5.5	Medium
CVE-2024-20799	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-04-02	5.4	Medium
CVE-2024-20302	Cisco	A vulnerability in the tenant security implementation of Cisco Nexus Dashboard Orchestrator (NDO) could allow an authenticated, remote attacker to modify or delete tenant templates on an affected system. This vulnerability is due to improper access controls within tenant security. An attacker who is using a valid user account with write privileges and either a Site Manager or Tenant Manager role could exploit this vulnerability. A successful exploit could allow the attacker to modify or delete tenant templates under non-associated tenants, which could disrupt network traffic.	2024-04-03	5.4	Medium
CVE-2024-20367	Cisco	A vulnerability in the web UI of Cisco Enterprise Chat and Email (ECE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web UI does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To successfully exploit this vulnerability, an attacker would need valid agent credentials.	2024-04-03	5.4	Medium
CVE-2024-20800	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution within the context of the victim's browser.	2024-04-04	5.4	Medium
CVE-2023-52296	IBM	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service when querying a specific UDF built-in function concurrently. IBM X-Force ID: 278547.	2024-04-03	5.3	Medium
CVE-2024-22360	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to a denial of service with a specially crafted query on certain columnar tables. IBM X-Force ID: 280905.	2024-04-03	5.3	Medium
CVE-2024-25046	IBM	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to a denial of service by an authenticated user using a specially crafted query. IBM X-Force ID: 282953.	2024-04-03	5.3	Medium
CVE-2024-27254	IBM	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 federated server is vulnerable to denial of service with a specially crafted query under certain conditions. IBM X-Force ID: 283813.	2024-04-03	5.3	Medium
CVE-2024-3274	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-320L, DNS-320LW and DNS-327L up to 20240403 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/info.cgi of the component HTTP GET Request Handler. The manipulation leads to information disclosure. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-259285 was assigned to this vulnerability. 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.	2024-04-04	5.3	Medium
CVE-2024-22023	Ivanti	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.	2024-04-04	5.3	Medium

CVE-2024-27910	Lenovo	A vulnerability was reported in some Lenovo Printers that could allow an unauthenticated attacker to reboot the printer without authentication.	2024-04-05	5.3	Medium
CVE-2023-50311	IBM	IBM CICS Transaction Gateway for Multiplatforms 9.2 and 9.3 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 273612.	2024-03-31	4.9	Medium
CVE-2024-20352	Cisco	A vulnerability in Cisco Emergency Responder could allow an authenticated, remote attacker to conduct a directory traversal attack, which could allow the attacker to perform arbitrary actions on an affected device. This vulnerability is due to insufficient protections for the web UI of an affected system. An attacker could exploit this vulnerability by sending crafted requests to the web UI. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user, such as accessing password or log files or uploading and deleting existing files from the system.	2024-04-03	4.9	Medium
CVE-2024-27908	Lenovo	A buffer overflow vulnerability was reported in the HTTPS service of some Lenovo Printers that could result in denial of service.	2024-04-05	4.9	Medium
CVE-2024-27909	Lenovo	A denial of service vulnerability was reported in the HTTPS service of some Lenovo Printers that could result in a system reboot.	2024-04-05	4.9	Medium
CVE-2024-20283	Cisco	A vulnerability in Cisco Nexus Dashboard could allow an authenticated, remote attacker to learn cluster deployment information on an affected device. This vulnerability is due to improper access controls on a specific API endpoint. An attacker could exploit this vulnerability by sending queries to the API endpoint. A successful exploit could allow an attacker to access metrics and information about devices in the Nexus Dashboard cluster.	2024-04-03	4.3	Medium
CVE-2024-20347	Cisco	A vulnerability in Cisco Emergency Responder could allow an unauthenticated, remote attacker to conduct a CSRF attack, which could allow the attacker to perform arbitrary actions on an affected device. This vulnerability is due to insufficient protections for the web UI of an affected system. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user, such as deleting users from the device.	2024-04-03	4.3	Medium
CVE-2024-29981	Microsoft	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-04-04	4.3	Medium
CVE-2024-29049	Microsoft	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability	2024-04-04	4.1	Medium
CVE-2024-29948	Hikvision	There is an out-of-bounds read vulnerability in some Hikvision NVRs. An authenticated attacker could exploit this vulnerability by sending specially crafted messages to a vulnerable device, causing a service abnormality.	2024-04-02	3.8	Low
CVE-2017-20191	Zimbra	A vulnerability was found in Zimbra zm-admin-ajax up to 8.8.1. It has been classified as problematic. This affects the function XFormItem.prototype.setError of the file WebRoot/js/ajax/dwt/xforms/XFormItem.js of the component Form Textbox Field Error Handler. The manipulation of the argument message leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 8.8.2 is able to address this issue. The identifier of the patch is bb240ce0c71c01caabaa43eed30c78ba8d7d3591. It is recommended to upgrade the affected component. The identifier VDB-258621 was assigned to this vulnerability.	2024-03-31	3.5	Low
CVE-2024-29947	Hikvision	There is a NULL dereference pointer vulnerability in some Hikvision NVRs. Due to an insufficient validation of a parameter in a message, an attacker may send specially crafted messages to an affected product, causing a process abnormality.	2024-04-02	2.7	Low

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.