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 ٧ اكتوبر إلى ١٣ اكتوبر. 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 7th of October to 13th of October. 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-2024-9463	paloaltonetworks - expedition	An OS command injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.	2024-10-09	9.9	Critical
CVE-2024-33066	qualcomm - snapdragon_x65_5g_modem-rf_system_firmware	Memory corruption while redirecting log file to any file location with any file name.	2024-10-07	9.8	Critical
CVE-2024-47009	ivanti - avalanche	Path Traversal in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to bypass authentication.	2024-10-08	9.8	Critical
CVE-2024-47010	ivanti - avalanche	Path Traversal in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to bypass authentication.	2024-10-08	9.8	Critical
CVE-2024-43468	microsoft - Microsoft Configuration Manager	Microsoft Configuration Manager Remote Code Execution Vulnerability	2024-10-08	9.8	Critical
CVE-2024-9680	mozilla - multiple products	An attacker was able to achieve code execution in the content process by exploiting a use-after-free in Animation timelines. We have had reports of this vulnerability being exploited in the wild. This vulnerability affects Firefox < 131.0.2, Firefox ESR < 128.3.1, Firefox ESR < 115.16.1, Thunderbird < 131.0.1, Thunderbird < 128.3.1, and Thunderbird < 115.16.0.	2024-10-09	9.8	Critical
CVE-2024-45115	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction.	2024-10-10	9.8	Critical
CVE-2024-47553	siemens - sinec_security_monitor	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate user input to the ```ssmctl-client``` command. This could allow an authenticated, lowly privileged remote attacker to execute arbitrary code with root privileges on the underlying OS.	2024-10-08	9.4	Critical
CVE-2023-52952	siemens - multiple products	A vulnerability has been identified in HiMed Cockpit 12 pro (J31032-K2017-H259) (All versions >= V11.5.1 < V11.6.2), HiMed Cockpit 14 pro+ (J31032-K2017-H435) (All versions >= V11.5.1 < V11.6.2), HiMed Cockpit 18 pro (J31032-K2017-H260) (All versions >= V11.5.1 < V11.6.2), HiMed Cockpit 18 pro+ (J31032-K2017-H436) (All versions >= V11.5.1 < V11.6.2). The Kiosk Mode of the affected devices contains a restricted desktop environment escape vulnerability. This could allow an unauthenticated local attacker to escape the restricted environment and gain access to the underlying operating system.	2024-10-08	9.3	Critical
CVE-2024-41798	siemens - SENTRON 7KM PAC3200	A vulnerability has been identified in SENTRON 7KM PAC3200 (All versions). Affected devices only provide a 4-digit PIN to protect from administrative access via Modbus TCP interface. Attackers with access to the Modbus TCP interface could easily bypass this protection by	2024-10-08	9.3	Critical

		brute-force attacks or by sniffing the Modbus clear text communication.			
CVE-2024-47562	siemens - sinec_security_monitor	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly neutralize special elements in user input to the ```ssmctl-client``` command. This could allow an authenticated, lowly privileged local attacker to execute privileged commands in the underlying OS.	2024-10-08	9.3	Critical
CVE-2024-9464	paloaltonetworks - expedition	An OS command injection vulnerability in Palo Alto Networks Expedition allows an authenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.	2024-10-09	9.3	Critical
CVE-2024-9465	paloaltonetworks - expedition	An SQL injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to reveal Expedition database contents, such as password hashes, usernames, device configurations, and device API keys. With this, attackers can also create and read arbitrary files on the Expedition system.	2024-10-09	9.2	Critical
CVE-2024-43591	microsoft - multiple products	Azure Command Line Integration (CLI) Elevation of Privilege Vulnerability	2024-10-08	9.1	Critical
CVE-2024-38124	microsoft - multiple products	Windows Netlogon Elevation of Privilege Vulnerability	2024-10-08	9	Critical
CVE-2024-8912	google - multiple products	An HTTP Request Smuggling vulnerability in Looker allowed an unauthorized attacker to capture HTTP responses destined for legitimate users. There are two Looker versions that are hosted by Looker: * Looker (Google Cloud core) was found to be vulnerable. This issue has already been mitigated and our investigation has found no signs of exploitation. * Looker (original) was not vulnerable to this issue. Customer-hosted Looker instances were found to be vulnerable and must be upgraded. This vulnerability has been patched in all supported versions of customer-hosted Looker, which are available on the Looker download page https://download.looker.com/ . For Looker customer-hosted instances, please update to the latest supported version of Looker as soon as possible. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page: * 23.12 -> 23.12.123+ * 23.18 -> 23.18.117+ * 24.0 -> 24.0.92+ * 24.6 -> 24.6.77+ * 24.8 -> 24.8.66+ * 24.10 -> 24.10.78+ * 24.12 -> 24.12.56+ * 24.14 -> 24.14.37+	2024-10-11	8.9	High
CVE-2024-7612	ivanti - Endpoint Manager Mobile	Insecure permissions in Ivanti EPMM before 12.1.0.4 allow a local authenticated attacker to modify sensitive application components.	2024-10-08	8.8	High
CVE-2024-38179	microsoft - multiple products	Azure Stack Hyperconverged Infrastructure (HCI) Elevation of Privilege Vulnerability	2024-10-08	8.8	High
CVE-2024-38212	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-38265	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43453	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43481	microsoft - power_bi_report_server	Power BI Report Server Spoofing Vulnerability	2024-10-08	8.8	High
CVE-2024-43488	microsoft - Visual Studio Code	Missing authentication for critical function in Visual Studio Code extension for Arduino allows an unauthenticated attacker to perform remote code execution through network attack vector.	2024-10-08	8.8	High
CVE-2024-43517	microsoft - multiple products	Microsoft ActiveX Data Objects Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43518	microsoft - multiple products	Windows Telephony Server Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43519	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43532	microsoft - multiple products	Remote Registry Service Elevation of Privilege Vulnerability	2024-10-08	8.8	High
CVE-2024-43533	microsoft - multiple products	Remote Desktop Client Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43549	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43564	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43589	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High

CVE-2024-43592	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43593	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43599	microsoft - multiple products	Remote Desktop Client Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43607	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43608	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-43611	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	8.8	High
CVE-2024-9602	google - Chrome	Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2024-10-08	8.8	High
CVE-2024-9603	google - Chrome	Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-10-08	8.8	High
CVE-2024-45148	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to gain unauthorized access without proper credentials. Exploitation of this issue does not require user interaction.	2024-10-10	8.8	High
CVE-2024-9859	google - Chrome	Type confusion in WebAssembly in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2024-10-11	8.8	High
CVE-2024-43584	microsoft - multiple products	Windows Scripting Engine Security Feature Bypass Vulnerability	2024-10-08	8.4	High
CVE-2024-43574	microsoft - multiple products	Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability	2024-10-08	8.3	High
CVE-2024-33064	qualcomm - qca6574au_firmware	Information disclosure while parsing the multiple MBSSID IEs from the beacon.	2024-10-07	8.2	High
CVE-2024-33073	qualcomm - wsa8845h_firmware	Information disclosure while parsing the BSS parameter change count or MLD capabilities fields of the ML IE.	2024-10-07	8.2	High
CVE-2024-43364	cacti - cacti	Cacti is an open source performance and fault management framework. The `title` parameter is not properly sanitized when saving external links in links.php . Morever, the said title parameter is stored in the database and reflected back to user in index.php, finally leading to stored XSS. Users with the privilege to create external links can manipulate the `title` parameter in the http post request while creating external links to perform stored XSS attacks. The vulnerability known as XSS (Cross-Site Scripting) occurs when an application allows untrusted user input to be displayed on a web page without proper validation or escaping. This issue has been addressed in release version 1.2.28. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-10-07	8.2	High
CVE-2024-43365	cacti - cacti	Cacti is an open source performance and fault management framework. The`consolenewsection` parameter is not properly sanitized when saving external links in links.php . Morever, the said consolenewsection parameter is stored in the database and reflected back to user in `index.php`, finally leading to stored XSS. Users with the privilege to create external links can manipulate the “consolenewsection” parameter in the http post request while creating external links to perform stored XSS attacks. The vulnerability known as XSS (Cross-Site Scripting) occurs when an application allows untrusted user input to be displayed on a web page without proper validation or escaping. This issue has been addressed in release version 1.2.28. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-10-07	8.2	High
CVE-2024-45720	apache software foundation - Apache Subversion	On Windows platforms, a "best fit" character encoding conversion of command line arguments to Subversion's executables (e.g., svn.exe, etc.) may lead to unexpected command line argument interpretation, including argument injection and execution of other programs, if a specially crafted command line argument string is processed. All versions of Subversion up to and including Subversion 1.14.3 are affected on Windows platforms only. Users are recommended to upgrade to version Subversion 1.14.4, which fixes this issue. Subversion is not affected on UNIX-like platforms.	2024-10-09	8.2	High
CVE-2024-9466	paloaltonetworks - expedition	A cleartext storage of sensitive information vulnerability in Palo Alto Networks Expedition allows an authenticated attacker to reveal firewall usernames, passwords, and API keys generated using those credentials.	2024-10-09	8.2	High
CVE-2024-38229	microsoft - multiple products	.NET and Visual Studio Remote Code Execution Vulnerability	2024-10-08	8.1	High
CVE-2024-43573	microsoft - multiple products	Windows MSHTML Platform Spoofing Vulnerability	2024-10-08	8.1	High
CVE-2024-43582	microsoft - multiple products	Remote Desktop Protocol Server Remote Code Execution Vulnerability	2024-10-08	8.1	High

CVE-2024-3656	red hat - multiple products	A flaw was found in Keycloak. Certain endpoints in Keycloak's admin REST API allow low-privilege users to access administrative functionalities. This flaw allows users to perform actions reserved for administrators, potentially leading to data breaches or system compromise.	2024-10-09	8.1	High
CVE-2024-45116	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction.	2024-10-10	8.1	High
CVE-2024-30092	microsoft - multiple products	Windows Hyper-V Remote Code Execution Vulnerability	2024-10-08	8	High
CVE-2024-43604	microsoft - outlook	Outlook for Android Elevation of Privilege Vulnerability	2024-10-08	8	High
CVE-2024-21455	qualcomm - qualcomm_video_collaboration_vc1_platform_firmware	Memory corruption when a compat IOCTL call is followed by another IOCTL call from userspace to a driver.	2024-10-07	7.8	High
CVE-2024-23369	qualcomm - snapdragon_888\+_5g_mobile_platform_\(sm8350-ac\)_firmware	Memory corruption when invalid length is provided from HLOS for FRS/UDS request/response buffers.	2024-10-07	7.8	High
CVE-2024-33065	qualcomm - wsa8845h_firmware	Memory corruption while taking snapshot when an offset variable is set by camera driver.	2024-10-07	7.8	High
CVE-2024-38399	qualcomm - wsa8835_firmware	Memory corruption while processing user packets to generate page faults.	2024-10-07	7.8	High
CVE-2024-43047	qualcomm - fastconnect_6700_firmware	Memory corruption while maintaining memory maps of HLOS memory.	2024-10-07	7.8	High
CVE-2024-8422	schneider-electric - zelio_soft_2	CWE-416: Use After Free vulnerability exists that could cause arbitrary code execution, denial of service and loss of confidentiality & integrity when application user opens a malicious Zelio Soft 2 project file.	2024-10-08	7.8	High
CVE-2024-37979	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-37982	microsoft - multiple products	Windows Resume Extensible Firmware Interface Security Feature Bypass Vulnerability	2024-10-08	7.8	High
CVE-2024-38261	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-10-08	7.8	High
CVE-2024-43497	microsoft - deepspeed	DeepSpeed Remote Code Execution Vulnerability	2024-10-08	7.8	High
CVE-2024-43501	microsoft - multiple products	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43503	microsoft - multiple products	Microsoft SharePoint Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43504	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2024-10-08	7.8	High
CVE-2024-43505	microsoft - multiple products	Microsoft Office Visio Remote Code Execution Vulnerability	2024-10-08	7.8	High
CVE-2024-43509	microsoft - multiple products	Windows Graphics Component Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43514	microsoft - multiple products	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43516	microsoft - multiple products	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43527	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43528	microsoft - multiple products	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43551	microsoft - multiple products	Windows Storage Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43556	microsoft - multiple products	Windows Graphics Component Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43560	microsoft - multiple products	Microsoft Windows Storage Port Driver Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43563	microsoft - multiple products	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43572	microsoft - multiple products	Microsoft Management Console Remote Code Execution Vulnerability	2024-10-08	7.8	High
CVE-2024-43576	microsoft - multiple products	Microsoft Office Remote Code Execution Vulnerability	2024-10-08	7.8	High
CVE-2024-43583	microsoft - multiple products	Winlogon Elevation of Privilege Vulnerability	2024-10-08	7.8	High

CVE-2024-43590	microsoft - multiple products	Visual C++ Redistributable Installer Elevation of Privilege Vulnerability	2024-10-08	7.8	High
CVE-2024-43616	microsoft - multiple products	Microsoft Office Remote Code Execution Vulnerability	2024-10-08	7.8	High
CVE-2024-45146	adobe - dimension	Dimension versions 4.0.3 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45150	adobe - dimension	Dimension versions 4.0.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47410	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47411	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47412	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47413	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47414	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47415	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47416	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47417	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47418	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45138	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45139	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45140	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45141	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45142	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by a Write-what-where Condition vulnerability that could allow an attacker to execute arbitrary code in the context of the current user. This vulnerability allows an attacker to write a controlled value to an arbitrary memory location, potentially leading to code execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45143	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45144	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code	2024-10-09	7.8	High

		execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2024-45152	adobe - substance_3d_stager	Substance3D - Stager versions 3.0.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45136	adobe - multiple products	InCopy versions 19.4, 18.5.3 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue requires user interaction.	2024-10-09	7.8	High
CVE-2024-45137	adobe - multiple products	InDesign Desktop versions 19.4, 18.5.3 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by uploading a malicious file which, when executed, could run arbitrary code in the context of the server. Exploitation of this issue requires user interaction.	2024-10-09	7.8	High
CVE-2024-47421	adobe - multiple products	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47422	adobe - multiple products	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by inserting a malicious path into the search directories, which the application could unknowingly execute. This could allow the attacker to execute arbitrary code in the context of the current user. Exploitation of this issue requires user interaction.	2024-10-09	7.8	High
CVE-2024-47423	adobe - multiple products	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by uploading a malicious file which can be automatically processed or executed by the system. Exploitation of this issue requires user interaction.	2024-10-09	7.8	High
CVE-2024-47424	adobe - multiple products	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-47425	adobe - multiple products	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	7.8	High
CVE-2024-45316	sonicwall - Connect Tunnel	The Improper link resolution before file access ('Link Following') vulnerability in SonicWall Connect Tunnel (version 12.4.3.271 and earlier of Windows client) allows users with standard privileges to delete arbitrary folders and files, potentially leading to local privilege escalation attack.	2024-10-11	7.8	High
CVE-2024-33578	lenovo - Leyun	A DLL hijack vulnerability was reported in Lenovo Leyun that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-33579	lenovo - Baiying	A DLL hijack vulnerability was reported in Lenovo Baiying that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-33580	lenovo - Personal Cloud	A DLL hijack vulnerability was reported in Lenovo Personal Cloud that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-33581	lenovo - PC Manager AI intelligent scenario	A DLL hijack vulnerability was reported in Lenovo PC Manager AI intelligent scenario that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-33582	lenovo - Service Framework	A DLL hijack vulnerability was reported in Lenovo Service Framework that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-4089	lenovo - superfile	A DLL hijack vulnerability was reported in Lenovo Super File that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-4130	lenovo - app_store	A DLL hijack vulnerability was reported in Lenovo App Store that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-4131	lenovo - emulator	A DLL hijack vulnerability was reported in Lenovo Emulator that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-4132	lenovo - lock_screen	A DLL hijack vulnerability was reported in Lenovo Lock Screen that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-9046	lenovo - starstudio	A DLL hijack vulnerability was reported in Lenovo stARstudio that could allow a local attacker to execute code with elevated privileges.	2024-10-11	7.8	High
CVE-2024-45117	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability	2024-10-10	7.6	High

		impact on the service. Exploitation of this issue does not require user interaction and scope is changed.			
CVE-2024-33049	qualcomm - snapdragon_w5\+_gen_1_wearable_platform_firmware	Transient DOS while parsing noninheritance IE of Extension element when length of IE is 2 of beacon frame.	2024-10-07	7.5	High
CVE-2024-33069	qualcomm - wsa8835_firmware	Transient DOS when transmission of management frame sent by host is not successful and error status is received in the host.	2024-10-07	7.5	High
CVE-2024-33070	qualcomm - qca6574au_firmware	Transient DOS while parsing ESP IE from beacon/probe response frame.	2024-10-07	7.5	High
CVE-2024-33071	qualcomm - mdm9628_firmware	Transient DOS while parsing the MBSSID IE from the beacons when IE length is 0.	2024-10-07	7.5	High
CVE-2024-38397	qualcomm - snapdragon_8\+_gen_2_mobile_platform_firmware	Transient DOS while parsing probe response and assoc response frame.	2024-10-07	7.5	High
CVE-2024-47007	ivanti - avalanche	A NULL pointer dereference in WLAvalancheService.exe of Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to cause a denial of service.	2024-10-08	7.5	High
CVE-2024-47008	ivanti - avalanche	Server-side request forgery in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to leak sensitive information.	2024-10-08	7.5	High
CVE-2024-47011	ivanti - avalanche	Path Traversal in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to leak sensitive information	2024-10-08	7.5	High
CVE-2024-38029	microsoft - windows_server_2022_23h2	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	2024-10-08	7.5	High
CVE-2024-38129	microsoft - Windows Server 2022, 23H2 Edition (Server Core installation)	Windows Kerberos Elevation of Privilege Vulnerability	2024-10-08	7.5	High
CVE-2024-38149	microsoft - multiple products	BranchCache Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-38262	microsoft - multiple products	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-10-08	7.5	High
CVE-2024-43483	microsoft - multiple products	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43484	microsoft - multiple products	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43485	microsoft - multiple products	.NET and Visual Studio Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43506	microsoft - multiple products	BranchCache Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43512	microsoft - multiple products	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43515	microsoft - multiple products	Internet Small Computer Systems Interface (iSCSI) Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43521	microsoft - multiple products	Windows Hyper-V Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43541	microsoft - multiple products	Microsoft Simple Certificate Enrollment Protocol Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43544	microsoft - multiple products	Microsoft Simple Certificate Enrollment Protocol Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43545	microsoft - multiple products	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43562	microsoft - multiple products	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43565	microsoft - multiple products	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43567	microsoft - multiple products	Windows Hyper-V Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-43575	microsoft - multiple products	Windows Hyper-V Denial of Service Vulnerability	2024-10-08	7.5	High
CVE-2024-28168	apache software foundation - Apache XML Graphics FOP	Improper Restriction of XML External Entity Reference ('XXE') vulnerability in Apache XML Graphics FOP. This issue affects Apache XML Graphics FOP: 2.9. Users are recommended to upgrade to version 2.10, which fixes the issue.	2024-10-09	7.5	High
CVE-2024-43550	microsoft - multiple products	Windows Secure Channel Spoofing Vulnerability	2024-10-08	7.4	High
CVE-2024-43610	microsoft - Microsoft Copilot Studio	Exposure of Sensitive Information to an Unauthorized Actor in Copilot Studio allows a unauthenticated attacker to view sensitive information through network attack vector	2024-10-09	7.4	High
CVE-2024-41902	siemens - JT2Go	A vulnerability has been identified in JT2Go (All versions < V2406.0003). The affected application contains a stack-based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF	2024-10-08	7.3	High

		files. This could allow an attacker to execute code in the context of the current process.			
CVE-2024-41981	siemens - multiple products	A vulnerability has been identified in Simcenter Nastran 2306 (All versions), Simcenter Nastran 2312 (All versions), Simcenter Nastran 2406 (All versions < V2406.5000). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted BDF files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45463	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45464	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45465	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45466	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45467	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45468	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45469	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45470	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45471	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45472	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45473	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-45474	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	2024-10-08	7.3	High

CVE-2024-45475	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-47046	siemens - multiple products	A vulnerability has been identified in Simcenter Nastran 2306 (All versions), Simcenter Nastran 2312 (All versions), Simcenter Nastran 2406 (All versions < V2406.5000). The affected application is vulnerable to memory corruption while parsing specially crafted BDF files. This could allow an attacker to execute code in the context of the current process.	2024-10-08	7.3	High
CVE-2024-43529	microsoft - multiple products	Windows Print Spooler Elevation of Privilege Vulnerability	2024-10-08	7.3	High
CVE-2024-43552	microsoft - multiple products	Windows Shell Remote Code Execution Vulnerability	2024-10-08	7.3	High
CVE-2024-43571	microsoft - multiple products	Sudo for Windows Spoofing Vulnerability	2024-10-08	7.3	High
CVE-2024-43363	cacti - cacti	Cacti is an open source performance and fault management framework. An admin user can create a device with a malicious hostname containing php code and repeat the installation process (completing only step 5 of the installation process is enough, no need to complete the steps before or after it) to use a php file as the cacti log file. After having the malicious hostname end up in the logs (log poisoning), one can simply go to the log file url to execute commands to achieve RCE. This issue has been addressed in version 1.2.28 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-10-07	7.2	High
CVE-2024-45330	fortinet - multiple products	A use of externally-controlled format string in Fortinet FortiAnalyzer versions 7.4.0 through 7.4.3, 7.2.2 through 7.2.5 allows attacker to escalate its privileges via specially crafted requests.	2024-10-08	7.2	High
CVE-2024-9379	ivanti - endpoint_manager_cloud_services_appliance	SQL injection in the admin web console of Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to run arbitrary SQL statements.	2024-10-08	7.2	High
CVE-2024-9380	ivanti - endpoint_manager_cloud_services_appliance	An OS command injection vulnerability in the admin web console of Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to obtain remote code execution.	2024-10-08	7.2	High
CVE-2024-9381	ivanti - endpoint_manager_cloud_services_appliance	Path traversal in Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to bypass restrictions.	2024-10-08	7.2	High
CVE-2024-20659	microsoft - multiple products	Windows Hyper-V Security Feature Bypass Vulnerability	2024-10-08	7.1	High
CVE-2024-38097	microsoft - azure_monitor_agent	Azure Monitor Agent Elevation of Privilege Vulnerability	2024-10-08	7.1	High
CVE-2024-43502	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-10-08	7.1	High
CVE-2024-43581	microsoft - multiple products	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	2024-10-08	7.1	High
CVE-2024-43601	microsoft - visual_studio_code	Visual Studio Code for Linux Remote Code Execution Vulnerability	2024-10-08	7.1	High
CVE-2024-43615	microsoft - multiple products	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	2024-10-08	7.1	High
CVE-2024-9167	ivanti - Velocity License Server	Under specific circumstances, insecure permissions in Ivanti Velocity License Server before version 5.2 allows a local authenticated attacker to achieve local privilege escalation.	2024-10-08	7	High
CVE-2024-43511	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-10-08	7	High
CVE-2024-43522	microsoft - multiple products	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability	2024-10-08	7	High
CVE-2024-43535	microsoft - multiple products	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-10-08	7	High
CVE-2024-43553	microsoft - multiple products	NT OS Kernel Elevation of Privilege Vulnerability	2024-10-08	7	High
CVE-2024-43570	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-10-08	7	High
CVE-2024-9467	paloaltonetworks - expedition	A reflected XSS vulnerability in Palo Alto Networks Expedition enables execution of malicious JavaScript in the context of an authenticated Expedition user's browser if that user clicks on a malicious link, allowing phishing attacks that could lead to Expedition browser session theft.	2024-10-09	7	High
CVE-2024-46887	siemens - multiple products	The web server of affected devices do not properly authenticate user request to the '/ClientArea/RuntimeInfoData.mwsl' endpoint. This could allow an unauthenticated remote attacker to gain knowledge about current actual and configured maximum cycle times as well as about configured maximum communication load.	2024-10-08	6.9	Medium

CVE-2024-47563	siemens - sinec_security_monitor	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate a file path that is supplied to an endpoint intended to create CSR files. This could allow an unauthenticated remote attacker to create files in writable directories outside the intended location and thus compromise integrity of files in those writable directories.	2024-10-08	6.9	Medium
CVE-2024-43612	microsoft - Power BI Report Server - May 2024	Power BI Report Server Spoofing Vulnerability	2024-10-08	6.9	Medium
CVE-2024-43523	microsoft - multiple products	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-10-08	6.8	Medium
CVE-2024-43524	microsoft - multiple products	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-10-08	6.8	Medium
CVE-2024-43525	microsoft - multiple products	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-10-08	6.8	Medium
CVE-2024-43526	microsoft - multiple products	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-10-08	6.8	Medium
CVE-2024-43536	microsoft - multiple products	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-10-08	6.8	Medium
CVE-2024-43543	microsoft - multiple products	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-10-08	6.8	Medium
CVE-2024-23370	qualcomm - wsa8835_firmware	Memory corruption when a process invokes IOCTL calls from user-space to create a HAB virtual channel and another process invokes IOCTL calls to destroy the same.	2024-10-07	6.7	Medium
CVE-2024-23374	qualcomm - wsa8835_firmware	Memory corruption is possible when an attempt is made from userspace or console to write some haptics effects pattern to the haptics debugfs file.	2024-10-07	6.7	Medium
CVE-2024-23375	qualcomm - wsa8835_firmware	Memory corruption during the network scan request.	2024-10-07	6.7	Medium
CVE-2024-23376	qualcomm - wsa8835_firmware	Memory corruption while sending the persist buffer command packet from the user-space to the kernel space through the IOCTL call.	2024-10-07	6.7	Medium
CVE-2024-23378	qualcomm - srv1m_firmware	Memory corruption while invoking IOCTL calls for MSM module from the user space during audio playback and record.	2024-10-07	6.7	Medium
CVE-2024-23379	qualcomm - wsa8835_firmware	Memory corruption while unmapping the fastrpc map when two threads can free the same map in concurrent scenario.	2024-10-07	6.7	Medium
CVE-2024-37976	microsoft - multiple products	Windows Resume Extensible Firmware Interface Security Feature Bypass Vulnerability	2024-10-08	6.7	Medium
CVE-2024-37983	microsoft - multiple products	Windows Resume Extensible Firmware Interface Security Feature Bypass Vulnerability	2024-10-08	6.7	Medium
CVE-2024-39436	google - multiple products	In linkturbonative service, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	2024-10-09	6.7	Medium
CVE-2024-39437	google - multiple products	In linkturbonative service, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	2024-10-09	6.7	Medium
CVE-2024-39438	google - multiple products	In linkturbonative service, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	2024-10-09	6.7	Medium
CVE-2024-43480	microsoft - multiple products	Azure Service Fabric for Linux Remote Code Execution Vulnerability	2024-10-08	6.6	Medium
CVE-2024-43534	microsoft - multiple products	Windows Graphics Component Information Disclosure Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43537	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43538	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43540	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43542	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43555	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43557	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43558	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43559	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43561	microsoft - multiple products	Windows Mobile Broadband Driver Denial of Service Vulnerability	2024-10-08	6.5	Medium
CVE-2024-43609	microsoft - multiple products	Microsoft Office Spoofing Vulnerability	2024-10-08	6.5	Medium
CVE-2024-45118	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high	2024-10-10	6.5	Medium

		impact on integrity. Exploitation of this issue does not require user interaction.			
CVE-2024-45132	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction.	2024-10-10	6.5	Medium
CVE-2024-43513	microsoft - multiple products	BitLocker Security Feature Bypass Vulnerability	2024-10-08	6.4	Medium
CVE-2024-45119	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs and have a low impact on both confidentiality and integrity. Exploitation of this issue does not require user interaction and scope is changed.	2024-10-10	6.4	Medium
CVE-2024-38425	qualcomm - wsa8835_firmware	Information disclosure while sending implicit broadcast containing APP launch information.	2024-10-07	6.1	Medium
CVE-2024-45123	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-10-10	6.1	Medium
CVE-2024-43547	microsoft - multiple products	Windows Kerberos Information Disclosure Vulnerability	2024-10-08	5.9	Medium
CVE-2024-9469	paloaltonetworks - multiple products	A problem with a detection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices enables a user with Windows non-administrative privileges to disable the agent. This issue may be leveraged by malware to disable the Cortex XDR agent and then to perform malicious activity.	2024-10-09	5.7	Medium
CVE-2024-43546	microsoft - multiple products	Windows Cryptographic Information Disclosure Vulnerability	2024-10-08	5.6	Medium
CVE-2024-43500	microsoft - multiple products	Windows Resilient File System (ReFS) Information Disclosure Vulnerability	2024-10-08	5.5	Medium
CVE-2024-43508	microsoft - multiple products	Windows Graphics Component Information Disclosure Vulnerability	2024-10-08	5.5	Medium
CVE-2024-43554	microsoft - multiple products	Windows Kernel-Mode Driver Information Disclosure Vulnerability	2024-10-08	5.5	Medium
CVE-2024-43585	microsoft - multiple products	Code Integrity Guard Security Feature Bypass Vulnerability	2024-10-08	5.5	Medium
CVE-2024-43603	microsoft - multiple products	Visual Studio Collector Service Denial of Service Vulnerability	2024-10-08	5.5	Medium
CVE-2024-43614	microsoft - Microsoft Defender for Endpoint for Linux	Microsoft Defender for Endpoint for Linux Spoofing Vulnerability	2024-10-08	5.5	Medium
CVE-2024-20787	adobe - substance_3d_painter	Substance3D - Painter versions 10.0.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	5.5	Medium
CVE-2024-45145	adobe - multiple products	Lightroom Desktop versions 7.4.1, 13.5, 12.5.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	5.5	Medium
CVE-2024-47419	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	5.5	Medium
CVE-2024-47420	adobe - multiple products	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-10-09	5.5	Medium
CVE-2024-47661	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid overflow from uint32_t to uint8_t [WHAT & HOW] dmub_rb_cmd's ramping_boundary has size of uint8_t and it is assigned 0xFFFF. Fix it by changing it to uint8_t with value of 0xFF. This fixes 2 INTEGER_OVERFLOW issues reported by Coverity.	2024-10-09	5.5	Medium
CVE-2024-5474	lenovo - Dolby Vision Provisioning software	A potential information disclosure vulnerability was reported in Lenovo's packaging of Dolby Vision Provisioning software prior to version 2.0.0.2 that could allow a local attacker to read files on the	2024-10-11	5.5	Medium

		system with elevated privileges during installation of the package. Previously installed versions are not affected by this issue.			
CVE-2024-45153	adobe - Adobe Experience Manager	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged 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.	2024-10-07	5.4	Medium
CVE-2024-43362	cacti - cacti	Cacti is an open source performance and fault management framework. The `fileurl` parameter is not properly sanitized when saving external links in `links.php` . Morever, the said fileurl is placed in some html code which is passed to the `print` function in `link.php` and `index.php`, finally leading to stored XSS. Users with the privilege to create external links can manipulate the `fileurl` parameter in the http post request while creating external links to perform stored XSS attacks. The vulnerability known as XSS (Cross-Site Scripting) occurs when an application allows untrusted user input to be displayed on a web page without proper validation or escaping. This issue has been addressed in release version 1.2.28. All users are advised to upgrade. There are no known workarounds for this issue.	2024-10-07	5.4	Medium
CVE-2024-47194	siemens - modelsim	A vulnerability has been identified in ModelSim (All versions < V2024.3), Questa (All versions < V2024.3). vish2.exe in affected applications allows a specific DLL file to be loaded from the current working directory. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges in installations where administrators or processes with elevated privileges launch vish2.exe from a user-writable directory.	2024-10-08	5.4	Medium
CVE-2024-47195	siemens - modelsim	A vulnerability has been identified in ModelSim (All versions < V2024.3), Questa (All versions < V2024.3). gdb.exe in affected applications allows a specific executable file to be loaded from the current working directory. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges in installations where administrators or processes with elevated privileges launch gdb.exe from a user-writable directory.	2024-10-08	5.4	Medium
CVE-2024-47196	siemens - modelsim	A vulnerability has been identified in ModelSim (All versions < V2024.3), Questa (All versions < V2024.3). vsimk.exe in affected applications allows a specific tcl file to be loaded from the current working directory. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges in installations where administrators or processes with elevated privileges launch vsimk.exe from a user-writable directory.	2024-10-08	5.4	Medium
CVE-2024-45128	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction.	2024-10-10	5.4	Medium
CVE-2024-45131	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction.	2024-10-10	5.4	Medium
CVE-2024-47565	siemens - sinec_security_monitor	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate that user input complies with a list of allowed values. This could allow an authenticated remote attacker to compromise the integrity of the configuration of the affected application.	2024-10-08	5.3	Medium
CVE-2024-9620	red hat - Red Hat Ansible Automation Platform 2	A flaw was found in Event-Driven Automation (EDA) in Ansible Automation Platform (AAP), which lacks encryption of sensitive information. An attacker with network access could exploit this vulnerability by sniffing the plaintext data transmitted between the EDA and AAP. An attacker with system access could exploit this vulnerability by reading the plaintext data stored in EDA and AAP databases.	2024-10-08	5.3	Medium
CVE-2024-9621	red hat - Red Hat build of Apache Camel for Quarkus	A vulnerability was found in Quarkus CXF. Passwords and other secrets may appear in the application log in spite of the user configuring them to be hidden. This issue requires some special configuration to be vulnerable, such as SOAP logging enabled, application set client, and endpoint logging properties, and the attacker must have access to the application log.	2024-10-08	5.3	Medium
CVE-2024-9622	red hat - multiple products	A vulnerability was found in the resteasy-netty4 library arising from improper handling of HTTP requests using smuggling techniques. When an HTTP smuggling request with an ASCII control character is sent, it causes the Netty HttpObjectDecoder to transition into a BAD_MESSAGE state. As a result, any subsequent legitimate requests on the same connection are ignored, leading to client timeouts, which may impact systems using load balancers and expose them to risk.	2024-10-08	5.3	Medium
CVE-2024-9671	red hat - Red Hat 3scale API	A vulnerability was found in 3Scale. There is no auth mechanism to see a PDF invoice of a Developer user if the URL is known. Anyone can see the invoice if the URL is known or guessed.	2024-10-09	5.3	Medium

	Management Platform 2				
CVE-2024-45124	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	2024-10-10	5.3	Medium
CVE-2024-9473	paloaltonetworks - multiple products	A privilege escalation vulnerability in the Palo Alto Networks GlobalProtect app on Windows allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY/SYSTEM through the use of the repair functionality offered by the .msi file used to install GlobalProtect.	2024-10-09	5.2	Medium
CVE-2024-46886	siemens - multiple products	The web server of affected devices does not properly validate input that is used for a user redirection. This could allow an attacker to make the server redirect the legitimate user to an attacker-chosen URL. For a successful exploit, the legitimate user must actively click on an attacker-crafted link.	2024-10-08	5.1	Medium
CVE-2024-9471	paloaltonetworks - multiple products	A privilege escalation (PE) vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated PAN-OS administrator with restricted privileges to use a compromised XML API key to perform actions as a higher privileged PAN-OS administrator. For example, an administrator with "Virtual system administrator (read-only)" access could use an XML API key of a "Virtual system administrator" to perform write operations on the virtual system configuration even though they should be limited to read-only operations.	2024-10-09	5.1	Medium
CVE-2024-9792	d-link - DSL-2750U	A vulnerability classified as problematic has been found in D-Link DSL-2750U R5B017. This affects an unknown part of the component Port Forwarding Page. The manipulation of the argument PortMappingDescription leads to cross site scripting. It is possible to initiate the attack remotely.	2024-10-10	5.1	Medium
CVE-2024-43520	microsoft - multiple products	Windows Kernel Denial of Service Vulnerability	2024-10-08	5	Medium
CVE-2024-20102	google - multiple products	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601.	2024-10-07	4.9	Medium
CVE-2024-45476	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted WRL files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-10-08	4.8	Medium
CVE-2024-43456	microsoft - multiple products	Windows Remote Desktop Services Tampering Vulnerability	2024-10-08	4.8	Medium
CVE-2024-45127	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin 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.	2024-10-10	4.8	Medium
CVE-2024-20091	google - android	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701.	2024-10-07	4.4	Medium
CVE-2024-20093	google - android	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699.	2024-10-07	4.4	Medium
CVE-2024-20095	google - multiple products	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636.	2024-10-07	4.4	Medium
CVE-2024-20096	google - multiple products	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635.	2024-10-07	4.4	Medium
CVE-2024-20097	google - android	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630.	2024-10-07	4.4	Medium
CVE-2024-39439	google - multiple products	In DRM service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2024-10-09	4.4	Medium
CVE-2024-39440	google - multiple products	In DRM service, there is a possible system crash due to null pointer dereference. This could lead to local denial of service with System execution privileges needed.	2024-10-09	4.4	Medium
CVE-2024-9675	red hat - multiple products	A vulnerability was found in Buildah. Cache mounts do not properly validate that user-specified paths for the cache are within our cache	2024-10-09	4.4	Medium

		directory, allowing a `RUN` instruction in a Container file to mount an arbitrary directory from the host (read/write) into the container as long as those files can be accessed by the user running Buildah.			
CVE-2024-39586	dell - emc_appsync	Dell AppSync Server, version 4.3 through 4.6, contains an XML External Entity Injection vulnerability. An adjacent high privileged attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-10-09	4.3	Medium
CVE-2024-45121	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	2024-10-10	4.3	Medium
CVE-2024-45122	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction.	2024-10-10	4.3	Medium
CVE-2024-45125	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction.	2024-10-10	4.3	Medium
CVE-2024-45129	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	2024-10-10	4.3	Medium
CVE-2024-45130	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	2024-10-10	4.3	Medium
CVE-2024-45149	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction.	2024-10-10	4.3	Medium
CVE-2024-33506	fortinet - FortiManager	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiManager 7.4.2 and below, 7.2.5 and below, 7.0.12 and below allows a remote authenticated attacker assigned to an Administrative Domain (ADOM) to access device summary of unauthorized ADOMs via crafted HTTP requests.	2024-10-08	3.3	Low
CVE-2024-45120	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction.	2024-10-10	3.1	Low
CVE-2024-45133	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction.	2024-10-10	2.7	Low
CVE-2024-45134	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction.	2024-10-10	2.7	Low
CVE-2024-45135	adobe - multiple products	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	2024-10-10	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.