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 ١٤ ابريل إلى ٢٠ 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 14th of April to 20th 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-2024-24996	Ivanti	A Heap overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows an unauthenticated remote attacker to execute arbitrary commands.	2024-04-19	9.8	Critical
CVE-2024-29204	Ivanti	A Heap Overflow vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows a remote unauthenticated attacker to execute arbitrary commands	2024-04-19	9.8	Critical
CVE-2023-4856	Lenovo	A format string vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user to execute arbitrary commands on a specific API endpoint.	2024-04-15	8.8	High
CVE-2024-3834	Google	Use after free in Downloads in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-04-17	8.8	High
CVE-2024-3837	Google	Use after free in QUIC in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-04-17	8.8	High
CVE-2024-23534	Ivanti	An Unrestricted File-upload vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-23535	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-24992	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-24993	Ivanti	A Race Condition (TOCTOU) vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-24994	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-24995	Ivanti	A Race Condition (TOCTOU) vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-24997	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-24998	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-24999	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-25000	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High

CVE-2024-27975	Ivanti	An Use-after-free vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-27976	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to execute arbitrary commands as SYSTEM.	2024-04-19	8.8	High
CVE-2024-28073	SolarWinds	SolarWinds Serv-U was found to be susceptible to a Directory Traversal Remote Code Vulnerability. This vulnerability requires a highly privileged account to be exploited.	2024-04-17	8.4	High
CVE-2024-21989	NetApp	ONTAP Select Deploy administration utility versions 9.12.1.x, 9.13.1.x and 9.14.1.x are susceptible to a vulnerability which when successfully exploited could allow a read-only user to escalate their privileges.	2024-04-17	8.1	High
CVE-2024-22061	Ivanti	A Heap Overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows a remote unauthenticated attacker to execute arbitrary commands	2024-04-19	8.1	High
CVE-2023-37400	IBM	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to escalate their privileges due to insecure credential storage. IBM X-Force ID: 259677.	2024-04-19	7.8	High
CVE-2023-4857	Lenovo	An authentication bypass vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user to execute certain IPMI calls that could lead to exposure of limited system information.	2024-04-15	7.5	High
CVE-2024-31887	IBM	IBM Security Verify Privilege 11.6.25 could allow an unauthenticated actor to obtain sensitive information from the SOAP API. IBM X-Force ID: 287651.	2024-04-16	7.5	High
CVE-2024-20380	Cisco	A vulnerability in the HTML parser of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an issue in the C to Rust foreign function interface. An attacker could exploit this vulnerability by submitting a crafted file containing HTML content to be scanned by ClamAV on an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2024-04-18	7.5	High
CVE-2024-23531	Ivanti	An Integer Overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows an unauthenticated remote attacker to perform denial of service attacks. In certain rare conditions this could also lead to reading content from memory.	2024-04-19	7.5	High
CVE-2024-23532	Ivanti	An out-of-bounds Read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows an authenticated remote attacker to perform denial of service attacks. In certain conditions this could also lead to remote code execution.	2024-04-19	7.5	High
CVE-2023-4855	Lenovo	A command injection vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user with elevated privileges to execute unauthorized commands via IPMI.	2024-04-15	7.2	High
CVE-2024-2659	Lenovo	A command injection vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user with elevated privileges to execute system commands when performing a specific administrative function.	2024-04-15	7.2	High
CVE-2024-27977	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to delete arbitrary files, thereby leading to Denial-of-Service.	2024-04-19	7.1	High
CVE-2024-27984	Ivanti	A Path Traversal vulnerability in web component of Ivanti Avalanche before 6.4.3 allows a remote authenticated attacker to delete specific type of files and/or cause denial of service.	2024-04-19	7.1	High
CVE-2024-22354	IBM	IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.3 are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information, consume memory resources, or to conduct a server-side request forgery attack. IBM X-Force ID: 280401.	2024-04-17	7	High
CVE-2024-23593	Lenovo	A vulnerability was reported in a system recovery bootloader that was part of the Lenovo preloaded Windows 7 and 8 operating systems from 2012 to 2014 that could allow a privileged attacker with local access to modify the boot manager and escalate privileges.	2024-04-15	6.7	Medium
CVE-2024-3839	Google	Out of bounds read in Fonts in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to obtain potentially	2024-04-17	6.5	Medium

		sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)			
CVE-2024-29987	Microsoft	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-04-18	6.5	Medium
CVE-2024-24991	Ivanti	A Null Pointer Dereference vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows an authenticated remote attacker to perform denial of service attacks.	2024-04-19	6.5	Medium
CVE-2024-27978	Ivanti	A Null Pointer Dereference vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows an authenticated remote attacker to perform denial of service attacks.	2024-04-19	6.5	Medium
CVE-2023-27279	IBM	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a user to cause a denial of service due to missing API rate limiting. IBM X-Force ID: 248533.	2024-04-19	6.5	Medium
CVE-2024-23594	Lenovo	A buffer overflow vulnerability was reported in a system recovery bootloader that was part of the Lenovo preloaded Windows 7 and 8 operating systems from 2012 to 2014 that could allow a privileged attacker with local access to execute arbitrary code.	2024-04-15	6.4	Medium
CVE-2024-3838	Google	Inappropriate implementation in Autofill in Google Chrome prior to 124.0.6367.60 allowed an attacker who convinced a user to install a malicious app to perform UI spoofing via a crafted app. (Chromium security severity: Medium)	2024-04-17	5.5	Medium
CVE-2023-22869	IBM	IBM Aspera Faspex 5.0.0 through 5.0.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 244119.	2024-04-19	5.5	Medium
CVE-2022-40745	IBM	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain sensitive information due to weaker than expected security. IBM X-Force ID: 236452.	2024-04-19	5.5	Medium
CVE-2024-21990	NetApp	ONTAP Select Deploy administration utility versions 9.12.1.x, 9.13.1.x and 9.14.1.x contain hard-coded credentials that could allow an attacker to view Deploy configuration information and modify the account credentials.	2024-04-17	5.4	Medium
CVE-2024-29986	Microsoft	Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability	2024-04-18	5.4	Medium
CVE-2024-24862	Linux	In function pci1xxxx_spi_probe, there is a potential null pointer that may be caused by a failed memory allocation by the function devm_kzalloc. Hence, a null pointer check needs to be added to prevent null pointer dereferencing later in the code. To fix this issue, spi_bus->spi_int[iter] should be checked. The memory allocated by devm_kzalloc will be automatically released, so just directly return -ENOMEM without worrying about memory leaks.	2024-04-14	5.3	Medium
CVE-2024-24863	Linux	In malidp_mw_connector_reset, new memory is allocated with kzalloc, but no check is performed. In order to prevent null pointer dereferencing, ensure that mw_state is checked before calling __drm_atomic_helper_connector_reset.	2024-04-14	5.3	Medium
CVE-2024-24856	Linux	The memory allocation function ACPI_ALLOCATE_ZEROED does not guarantee a successful allocation, but the subsequent code directly dereferences the pointer that receives it, which may lead to null pointer dereference. To fix this issue, a null pointer check should be added. If it is null, return exception code AE_NO_MEMORY.	2024-04-17	5.3	Medium
CVE-2024-23526	Ivanti	An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions can allow an unauthenticated remote attacker to read sensitive information in memory.	2024-04-19	5.3	Medium
CVE-2024-23528	Ivanti	An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions	2024-04-19	5.3	Medium

		can allow an unauthenticated remote attacker to read sensitive information in memory.			
CVE-2024-23529	Ivanti	An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions can allow an unauthenticated remote attacker to read sensitive information in memory.	2024-04-19	5.3	Medium
CVE-2024-23530	Ivanti	An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions can allow an unauthenticated remote attacker to read sensitive information in memory.	2024-04-19	5.3	Medium
CVE-2024-29991	Microsoft	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-04-19	5	Medium
CVE-2024-22329	IBM	IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.3 are vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker could exploit this vulnerability to conduct the SSRF attack. X-Force ID: 279951.	2024-04-17	4.3	Medium
CVE-2024-23533	Ivanti	An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions can allow an authenticated remote attacker to read sensitive information in memory.	2024-04-19	4.3	Medium
CVE-2023-37397	IBM	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain or modify sensitive information due to improper encryption of certain data. IBM X-Force ID: 259672.	2024-04-19	3.6	Low
CVE-2023-37396	IBM	IBM Aspera Faspex 5.0.0 through 5.0.7 could allow a local user to obtain sensitive information due to improper encryption of certain data. IBM X-Force ID: 259671.	2024-04-19	2.5	Low

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.

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.

متاح