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 ٢٧ أغسطس إلى ٣ سبتمبر. 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 27th of August to 3rd of September. 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-2023-26270	ibm - guardium_cloud_key_manager	IBM Security Guardium Data Encryption (IBM Guardium Cloud Key Manager (GCKM) 1.10.3)) could allow a remote attacker to execute arbitrary code on the system, caused by an angular template injection flaw. By sending specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 248119.	2023-08-28	9.8	Critical
CVE-2023-35785	zohocorp - multiple products	Zoho ManageEngine Active Directory 360 versions 4315 and below, ADAudit Plus 7202 and below, ADManager Plus 7200 and below, Asset Explorer 7002 and below, Cloud Security Plus 4161 and below, Data Security Plus 6110 and below, Eventlog Analyzer 12301 and below, Exchange Reporter Plus 5709 and below, Log360 5315 and below, Log360 UEBA 4045 and below, M365 Manager Plus 4529 and below, M365 Security Plus 4529 and below, Recovery Manager Plus 6061 and below, ServiceDesk Plus 14302 and below, ServiceDesk Plus MSP 14300 and below, SharePoint Manager Plus 4402 and below and Support Center Plus 14300 and below are vulnerable to the authentication bypass vulnerability via a few authenticators.	2023-08-28	9.8	Critical
CVE-2023-34039	vmware - aria_operations_for_networks	Aria Operations for Networks contains an Authentication Bypass vulnerability due to a lack of unique cryptographic key generation. A malicious actor with network access to Aria Operations for Networks could bypass SSH authentication to gain access to the Aria Operations for Networks CLI.	2023-08-29	9.8	Critical
CVE-2023-36187	netgear - cbr40_firmware	Buffer Overflow vulnerability in NETGEAR R6400v2 before version 1.0.4.118, allows remote unauthenticated attackers to execute arbitrary code via crafted URL to httpd.	2023-09-01	9.8	Critical
CVE-2022-43907	ibm - security_guardium	IBM Security Guardium 11.4 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 240901.	2023-08-27	8.8	High
CVE-2023-22877	ibm - multiple products	IBM InfoSphere Information Server 11.7 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 244368.	2023-08-28	8.8	High
CVE-2023-23473	ibm - multiple products	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 245400.	2023-08-28	8.8	High
CVE-2023-27604	apache - airflow_sqoop_provider	Apache Airflow Sqoop Provider, versions before 4.0.0, is affected by a vulnerability that allows an attacker pass parameters with the connections, which makes it possible to implement RCE attacks via 'sqoop import --connect', obtain airflow server permissions, etc. The attacker needs to be logged in and have authorization (permissions) to create/edit connections. It is recommended to upgrade to a version that is not affected. This issue was reported independently by happyhacking-k, And Xie Jianming and LiuHui of Caiji Sec Team also reported it.	2023-08-28	8.8	High

CVE-2023-40195	apache - airflow_spark_provider	Deserialization of Untrusted Data, Inclusion of Functionality from Untrusted Control Sphere vulnerability in Apache Software Foundation Apache Airflow Spark Provider. When the Apache Spark provider is installed on an Airflow deployment, an Airflow user that is authorized to configure Spark hooks can effectively run arbitrary code on the Airflow node by pointing it at a malicious Spark server. Prior to version 4.1.3, this was not called out in the documentation explicitly, so it is possible that administrators provided authorizations to configure Spark hooks without taking this into account. We recommend administrators to review their configurations to make sure the authorization to configure Spark hooks is only provided to fully trusted users. To view the warning in the docs please visit https://airflow.apache.org/docs/apache-airflow-providers-apache-spark/4.1.3/connections/spark.html	2023-08-28	8.8	High
CVE-2023-32457	dell - multiple products	Dell PowerScale OneFS, versions 8.2.2.x-9.5.0.x, contains an improper privilege management vulnerability. A remote attacker with low privileges could potentially exploit this vulnerability, leading to escalation of privileges.	2023-08-29	8.8	High
CVE-2023-4572	google - chrome	Use after free in MediaStream in Google Chrome prior to 116.0.5845.140 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-29	8.8	High
CVE-2023-41738	synology - router_manager	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in Directory Domain Functionality in Synology Router Manager (SRM) before 1.3.1-9346-6 allows remote authenticated users to execute arbitrary commands via unspecified vectors.	2023-08-31	8.8	High
CVE-2023-38730	ibm - storage_copy_data_management	IBM Storage Copy Data Management 2.2.0.0 through 2.2.19.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 262268.	2023-08-27	7.5	High
CVE-2022-43904	ibm - multiple products	IBM Security Guardium 11.3 and 11.4 could disclose sensitive information to an attacker due to improper restriction of excessive authentication attempts. IBM X-Force ID: 240895.	2023-08-28	7.5	High
CVE-2023-24959	ibm - multiple products	IBM InfoSphere Information Systems 11.7 could expose information about the host system and environment configuration. IBM X-Force ID: 246332.	2023-08-28	7.5	High
CVE-2023-26271	ibm - guardium_cloud_key_manager	IBM Security Guardium Data Encryption (IBM Guardium Cloud Key Manager (GCKM) 1.10.3)) uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 248126.	2023-08-28	7.5	High
CVE-2023-36481	samsung - exynos_9810_firmware	An issue was discovered in Samsung Exynos Mobile Processor and Wearable Processor 9810, 9610, 9820, 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, and W920. Improper handling of PPP length parameter inconsistency can cause an infinite loop.	2023-08-28	7.5	High
CVE-2021-32050	mongodb - multiple products	Some MongoDB Drivers may erroneously publish events containing authentication-related data to a command listener configured by an application. The published events may contain security-sensitive data when specific authentication-related commands are executed. Without due care, an application may inadvertently expose this sensitive information, e.g., by writing it to a log file. This issue only arises if an application enables the command listener feature (this is not enabled by default). This issue affects the MongoDB C Driver 1.0.0 prior to 1.17.7, MongoDB PHP Driver 1.0.0 prior to 1.9.2, MongoDB Swift Driver 1.0.0 prior to 1.1.1, MongoDB Node.js Driver 3.6 prior to 3.6.10, MongoDB Node.js Driver 4.0 prior to 4.17.0 and MongoDB Node.js Driver 5.0 prior to 5.8.0. This issue also affects users of the MongoDB C++ Driver dependent on the C driver 1.0.0 prior to 1.17.7 (C++ driver prior to 3.7.0).	2023-08-29	7.5	High
CVE-2023-20900	vmware - tools	A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html .	2023-08-31	7.5	High
CVE-2023-41741	synology - router_manager	Exposure of sensitive information to an unauthorized actor vulnerability in cgi component in Synology Router Manager (SRM)	2023-08-31	7.5	High

		before 1.3.1-9346-6 allows remote attackers to obtain sensitive information via unspecified vectors.			
CVE-2023-33835	ibm - multiple products	IBM Security Verify Information Queue 10.0.4 and 10.0.5 could allow a remote attacker to obtain sensitive information that could aid in further attacks against the system. IBM X-Force ID: 256015.	2023-08-31	7.5	High
CVE-2023-4481	juniper - multiple products	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When certain specific crafted BGP UPDATE messages are received over an established BGP session, one BGP session may be torn down with an UPDATE message error, or the issue may propagate beyond the local system which will remain non-impacted, but may affect one or more remote systems. This issue is exploitable remotely as the crafted UPDATE message can propagate through unaffected systems and intermediate BGP speakers. Continuous receipt of the crafted BGP UPDATE messages will create a sustained Denial of Service (DoS) condition for impacted devices. This issue affects eBGP and iBGP, in both IPv4 and IPv6 implementations. This issue requires a remote attacker to have at least one established BGP session.	2023-09-01	7.5	High
CVE-2023-20890	vmware - aria_operations_for_networks	Aria Operations for Networks contains an arbitrary file write vulnerability. An authenticated malicious actor with administrative access to VMware Aria Operations for Networks can write files to arbitrary locations resulting in remote code execution.	2023-08-29	7.2	High
CVE-2023-41739	synology - router_manager	Uncontrolled resource consumption vulnerability in File Functionality in Synology Router Manager (SRM) before 1.3.1-9346-6 allows remote authenticated users to conduct denial-of-service attacks via unspecified vectors.	2023-08-31	6.5	Medium
CVE-2023-4611	linux - multiple products	A use-after-free flaw was found in mm/mempolicy.c in the memory management subsystem in the Linux Kernel. This issue is caused by a race between mbind() and VMA-locked page fault, and may allow a local attacker to crash the system or lead to a kernel information leak.	2023-08-29	6.3	Medium
CVE-2023-4569	linux - multiple products	A memory leak flaw was found in nft_set_catchall_flush in net/netfilter/nf_tables_api.c in the Linux Kernel. This issue may allow a local attacker to cause a double-deactivations of catchall elements, which results in a memory leak.	2023-08-28	5.5	Medium
CVE-2022-43909	ibm - security_guardium	IBM Security Guardium 11.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 240905.	2023-08-27	5.4	Medium
CVE-2023-30435	ibm - multiple products	IBM Security Guardium 11.3, 11.4, and 11.5 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 252291.	2023-08-27	5.4	Medium
CVE-2023-30436	ibm - multiple products	IBM Security Guardium 11.3, 11.4, and 11.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 252292.	2023-08-27	5.4	Medium
CVE-2023-33852	ibm - security_guardium	IBM Security Guardium 11.4 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 257614.	2023-08-27	5.4	Medium
CVE-2023-30437	ibm - multiple products	IBM Security Guardium 11.3, 11.4, and 11.5 could allow an unauthorized user to enumerate usernames by sending a specially crafted HTTP request. IBM X-Force ID: 252293.	2023-08-27	5.3	Medium
CVE-2023-26272	ibm - guardium_cloud_key_manager	IBM Security Guardium Data Encryption (IBM Guardium Cloud Key Manager (GCKM) 1.10.3)) could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 248133.	2023-08-28	5.3	Medium
CVE-2023-41740	synology - router_manager	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in cgi component in Synology Router Manager (SRM) before 1.3.1-9346-6 allows remote attackers to read specific files via unspecified vectors.	2023-08-31	5.3	Medium
CVE-2023-33834	ibm - multiple products	IBM Security Verify Information Queue 10.0.4 and 10.0.5 could allow a remote attacker to obtain sensitive information that could aid in further attacks against the system. IBM X-force ID: 256014.	2023-08-31	5.3	Medium
CVE-2023-39912	zohocorp - manageengine_admanager_plus	Zoho ManageEngine ADManager Plus through 7202 allows admin users to download any file from the server machine via directory traversal.	2023-08-31	4.9	Medium

CVE-2022-22305	fortinet - multiple products	An improper certificate validation vulnerability [CWE-295] in FortiManager 7.0.1 and below, 6.4.6 and below; FortiAnalyzer 7.0.2 and below, 6.4.7 and below; FortiOS 6.2.x and 6.0.x; FortiSandbox 4.0.x, 3.2.x and 3.1.x may allow a network adjacent and unauthenticated attacker to man-in-the-middle the communication between the listed products and some external peers.	2023-09-01	4.2	Medium
CVE-2023-33833	ibm - multiple products	IBM Security Verify Information Queue 10.0.4 and 10.0.5 stores sensitive information in plain clear text which can be read by a local user. IBM X-Force ID: 256013.	2023-08-31	3.3	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.
