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 24 مارس إلى 30 مارس. 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 24th of March to 30th of March. 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-2024-29241	Synology	Missing authorization vulnerability in System webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to bypass security constraints via unspecified vectors.	2024-03-28	9.9	Critical
CVE-2023-6437	TP-Link	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in TP-Link TP-Link EX20v AX1800, Tp-Link Archer C5v AC1200, Tp-Link TD-W9970, Tp-Link TD-W9970v3, TP-Link VX220-G2u, TP-Link VN020-G2u allows authenticated OS Command Injection.This issue affects TP-Link EX20v AX1800, Tp-Link Archer C5v AC1200, Tp-Link TD-W9970, Tp-Link TD-W9970v3 : through 20240328. Also the vulnerability continues in the TP-Link VX220-G2u and TP-Link VN020-G2u models due to the products not being produced and supported.	2024-03-28	9.8	Critical
CVE-2024-20259	Cisco	A vulnerability in the DHCP snooping feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a crafted IPv4 DHCP request packet being mishandled when endpoint analytics are enabled. An attacker could exploit this vulnerability by sending a crafted DHCP request through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: The attack vector is listed as network because a DHCP relay anywhere on the network could allow exploits from networks other than the adjacent one.	2024-03-27	8.6	High
CVE-2024-20271	Cisco	A vulnerability in the IP packet processing of Cisco Access Point (AP) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of certain IPv4 packets. An attacker could exploit this vulnerability by sending a crafted IPv4 packet either to or through an affected device. A successful exploit could allow the attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition. To successfully exploit this vulnerability, the attacker does not need to be associated with the affected AP. This vulnerability cannot be exploited by sending IPv6 packets.	2024-03-27	8.6	High
CVE-2024-20311	Cisco	A vulnerability in the Locator ID Separation Protocol (LISP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to the incorrect handling of LISP packets. An attacker could exploit this vulnerability by sending a crafted LISP packet to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition. Note: This vulnerability could be exploited over either IPv4 or IPv6 transport.	2024-03-27	8.6	High

CVE-2024-20314	Cisco	A vulnerability in the IPv4 Software-Defined Access (SD-Access) fabric edge node feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause high CPU utilization and stop all traffic processing, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain IPv4 packets. An attacker could exploit this vulnerability by sending certain IPv4 packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust CPU resources and stop processing traffic, resulting in a DoS condition.	2024-03-27	8.6	High
CVE-2024-20308	Cisco	A vulnerability in the IKEv1 fragmentation code of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a heap underflow, resulting in an affected device reloading. This vulnerability exists because crafted, fragmented IKEv1 packets are not properly reassembled. An attacker could exploit this vulnerability by sending crafted UDP packets to an affected system. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. Note: Only traffic that is directed to the affected system can be used to exploit this vulnerability. This vulnerability can be triggered by IPv4 and IPv6 traffic..	2024-03-27	8.6	High
CVE-2024-25962	Dell	Dell InsightIQ, version 5.0, contains an improper access control vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to unauthorized access to monitoring data.	2024-03-27	8.3	High
CVE-2024-25959	Dell	Dell PowerScale OneFS versions 9.4.0.x through 9.7.0.x contains an insertion of sensitive information into log file vulnerability. A low privileged local attacker could potentially exploit this vulnerability, leading to sensitive information disclosure, escalation of privileges.	2024-03-28	7.9	High
CVE-2024-29228	Synology	Missing authorization vulnerability in GetStmUrlPath webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to obtain sensitive information via unspecified vectors.	2024-03-28	7.7	High
CVE-2024-29229	Synology	Missing authorization vulnerability in GetLiveViewPath webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to obtain sensitive information via unspecified vectors.	2024-03-28	7.7	High
CVE-2024-28247	pi-hole	The Pi-hole is a DNS sinkhole that protects your devices from unwanted content without installing any client-side software. A vulnerability has been discovered in Pihole that allows an authenticated user on the platform to read internal server files arbitrarily, and because the application runs from behind, reading files is done as a privileged user.If the URL that is in the list of "Adslists" begins with "file*" it is understood that it is updating from a local file, on the other hand if it does not begin with "file*" depending on the state of the response it does one thing or another. The problem resides in the update through local files. When updating from a file which contains non-domain lines, 5 of the non-domain lines are printed on the screen, so if you provide it with any file on the server which contains non-domain lines it will print them on the screen. This vulnerability is fixed by 5.18.	2024-03-27	7.6	High
CVE-2023-47150	IBM	IBM Common Cryptographic Architecture (CCA) 7.0.0 through 7.5.36 could allow a remote user to cause a denial of service due to incorrect data handling for certain types of AES operations. IBM X-Force ID: 270602.	2024-03-26	7.5	High
CVE-2024-20276	Cisco	A vulnerability in Cisco IOS Software for Cisco Catalyst 6000 Series Switches could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly. This vulnerability is due to improper handling of process-switched traffic. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.	2024-03-27	7.4	High
CVE-2024-20303	Cisco	A vulnerability in the multicast DNS (mDNS) gateway feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper management of mDNS client entries. An attacker could exploit this vulnerability by connecting to the wireless network and sending a continuous stream of specific mDNS packets. A successful exploit could allow the attacker to cause the wireless controller to have high CPU utilization, which could lead to access points (APs) losing their connection to the controller and result in a DoS condition.	2024-03-27	7.4	High
CVE-2024-20312	Cisco	A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation when parsing an	2024-03-27	7.4	High

		ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device after forming an adjacency. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer 2-adjacent to the affected device and have formed an adjacency.			
CVE-2024-25960	Dell	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.x contains a cleartext transmission of sensitive information vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2024-03-28	7.3	High
CVE-2024-25946	Dell	Dell vApp Manager, versions prior to 9.2.4.9 contain a Command Injection Vulnerability. An authorized attacker could potentially exploit this vulnerability leading to an execution of an inserted command. Dell recommends customers to upgrade at the earliest opportunity.	2024-03-28	7.2	High
CVE-2024-25955	Dell	Dell vApp Manager, versions prior to 9.2.4.9 contain a Command Injection Vulnerability. An authorized attacker could potentially exploit this vulnerability leading to an execution of an inserted command. Dell recommends customers to upgrade at the earliest opportunity.	2024-03-28	7.2	High
CVE-2024-1933	TeamViewer	Insecure UNIX Symbolic Link (Symlink) Following in TeamViewer Remote Client prior Version 15.52 for macOS allows an attacker with unprivileged access, to potentially elevate privileges or conduct a denial-of-service-attack by overwriting the symlink.	2024-03-26	7.1	High
CVE-2024-20307	Cisco	A vulnerability in the IKEv1 fragmentation code of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a heap overflow, resulting in an affected device reloading. This vulnerability exists because crafted, fragmented IKEv1 packets are not properly reassembled. An attacker could exploit this vulnerability by sending crafted UDP packets to an affected system. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Only traffic that is directed to the affected system can be used to exploit this vulnerability. This vulnerability can be triggered by IPv4 and IPv6 traffic.	2024-03-27	6.8	Medium
CVE-2024-25958	Dell	Dell Grab for Windows, versions up to and including 5.0.4, contain Weak Application Folder Permissions vulnerability. A local authenticated attacker could potentially exploit this vulnerability, leading to privilege escalation, unauthorized access to application data, unauthorized modification of application data and service disruption.	2024-03-26	6.7	Medium
CVE-2024-1313	Grafana	It is possible for a user in a different organization from the owner of a snapshot to bypass authorization and delete a snapshot by issuing a DELETE request to /api/snapshots/<key> using its view key. This functionality is intended to only be available to individuals with the permission to write/edit to the snapshot in question, but due to a bug in the authorization logic, deletion requests issued by an unprivileged user in a different organization than the snapshot owner are treated as authorized. Grafana Labs would like to thank Ravid Mazon and Jay Chen of Palo Alto Research for discovering and disclosing this vulnerability. This issue affects Grafana: from 9.5.0 before 9.5.18, from 10.0.0 before 10.0.13, from 10.1.0 before 10.1.9, from 10.2.0 before 10.2.6, from 10.3.0 before 10.3.5.	2024-03-26	6.5	Medium
CVE-2024-20278	Cisco	A vulnerability in the NETCONF feature of Cisco IOS XE Software could allow an authenticated, remote attacker to elevate privileges to root on an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input over NETCONF to an affected device. A successful exploit could allow the attacker to elevate privileges from Administrator to root.	2024-03-27	6.5	Medium
CVE-2024-20306	Cisco	A vulnerability in the Unified Threat Defense (UTD) configuration CLI of Cisco IOS XE Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying host operating system. To exploit this vulnerability, an attacker must have level 15 privileges on the affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by submitting a crafted CLI command to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying operating system.	2024-03-27	6	Medium
CVE-2024-25961	Dell	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.x contains an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2024-03-28	6	Medium

CVE-2024-25952	Dell	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.x contains an UNIX symbolic link (symlink) following vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to denial of service, information tampering.	2024-03-28	6	Medium
CVE-2024-25953	Dell	Dell PowerScale OneFS versions 9.4.0.x through 9.7.0.x contains an UNIX symbolic link (symlink) following vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to denial of service, information tampering.	2024-03-28	6	Medium
CVE-2024-20265	Cisco	A vulnerability in the boot process of Cisco Access Point (AP) Software could allow an unauthenticated, physical attacker to bypass the Cisco Secure Boot functionality and load a software image that has been tampered with on an affected device. This vulnerability exists because unnecessary commands are available during boot time at the physical console. An attacker could exploit this vulnerability by interrupting the boot process and executing specific commands to bypass the Cisco Secure Boot validation checks and load an image that has been tampered with. This image would have been previously downloaded onto the targeted device. A successful exploit could allow the attacker to load the image once. The Cisco Secure Boot functionality is not permanently compromised.	2024-03-27	5.9	Medium
CVE-2024-25963	Dell	Dell PowerScale OneFS, versions 8.2.2.x through 9.5.0.x contains a use of a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-03-28	5.9	Medium
CVE-2024-20316	Cisco	A vulnerability in the data model interface (DMI) services of Cisco IOS XE Software could allow an unauthenticated, remote attacker to access resources that should have been protected by a configured IPv4 access control list (ACL). This vulnerability is due to improper handling of error conditions when a successfully authorized device administrator updates an IPv4 ACL using the NETCONF or RESTCONF protocol, and the update would reorder access control entries (ACEs) in the updated ACL. An attacker could exploit this vulnerability by accessing resources that should have been protected across an affected device.	2024-03-27	5.8	Medium
CVE-2024-25944	Dell	Dell OpenManage Enterprise, v4.0 and prior, contain(s) a path traversal vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, to gain unauthorized access to the files stored on the server filesystem, with the privileges of the running web application.	2024-03-29	5.7	Medium
CVE-2024-20309	Cisco	A vulnerability in auxiliary asynchronous port (AUX) functions of Cisco IOS XE Software could allow an authenticated, local attacker to cause an affected device to reload or stop responding. This vulnerability is due to the incorrect handling of specific ingress traffic when flow control hardware is enabled on the AUX port. An attacker could exploit this vulnerability by reverse telnetting to the AUX port and sending specific data after connecting. A successful exploit could allow the attacker to cause the device to reset or stop responding, resulting in a denial of service (DoS) condition.	2024-03-27	5.6	Medium
CVE-2024-25956	Dell	Dell Grab for Windows, versions 5.0.4 and below, contains an improper file permissions vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to the information disclosure of certain system information.	2024-03-26	5.5	Medium
CVE-2024-20324	Cisco	A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, low-privileged, local attacker to access WLAN configuration details including passwords. This vulnerability is due to improper privilege checks. An attacker could exploit this vulnerability by using the show and show tech wireless CLI commands to access configuration details, including passwords. A successful exploit could allow the attacker to access configuration details that they are not authorized to access.	2024-03-27	5.5	Medium
CVE-2024-25971	Dell	Dell PowerProtect Data Manager, version 19.15, contains an XML External Entity Injection vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to information disclosure, denial-of-service.	2024-03-28	5.5	Medium
CVE-2024-28784	IBM	IBM QRadar SIEM 7.5 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: 285893.	2024-03-27	5.4	Medium
CVE-2024-29227	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Layout.LayoutSave webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29230	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in SnapShot.CountByCategory webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows	2024-03-28	5.4	Medium

		remote authenticated users to inject SQL commands via unspecified vectors.			
CVE-2024-29231	Synology	Improper validation of array index vulnerability in UserPrivilege.Enum webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to bypass security constraints via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29232	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Alert.Enum webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29233	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Emap.Delete webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29234	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Group.Save webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29235	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in IOModule.EnumLog webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29236	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in AudioPattern.Delete webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29237	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in ActionRule.Delete webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29238	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Log.CountByCategory webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-29239	Synology	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Recording.CountByCategory webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	Medium
CVE-2024-25964	Dell	Dell PowerScale OneFS 9.5.0.x through 9.7.0.x contain a covert timing channel vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2024-03-25	5.3	Medium
CVE-2024-25954	Dell	Dell PowerScale OneFS, versions 9.5.0.x through 9.7.0.x, contain an insufficient session expiration vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2024-03-28	5.3	Medium
CVE-2024-22356	IBM	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.23, 12.0.1.0 through 12.0.9.0 and IBM Integration Bus for z/OS 10.1 through 10.1.0.2store potentially sensitive information in log or trace files that could be read by a privileged user. IBM X-Force ID: 280893.	2024-03-26	4.9	Medium
CVE-2024-25957	Dell	Dell Grab for Windows, versions 5.0.4 and below, contains a cleartext storage of sensitive information vulnerability in its appsync module. An authenticated local attacker could potentially exploit this vulnerability, leading to information disclosure that could be used to access the appsync application with elevated privileges.	2024-03-26	4.8	Medium
CVE-2023-50961	IBM	IBM QRadar SIEM 7.5 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: 275939.	2024-03-27	4.8	Medium
CVE-2024-27270	IBM	IBM WebSphere Application Server Liberty 23.0.0.3 through 24.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in a specially crafted URI. IBM X-Force ID: 284576.	2024-03-27	4.7	Medium
CVE-2024-20354	Cisco	A vulnerability in the handling of encrypted wireless frames of Cisco Aironet Access Point (AP) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on the affected device. This vulnerability is due to	2024-03-27	4.7	Medium

		incomplete cleanup of resources when dropping certain malformed frames. An attacker could exploit this vulnerability by connecting as a wireless client to an affected AP and sending specific malformed frames over the wireless connection. A successful exploit could allow the attacker to cause degradation of service to other clients, which could potentially lead to a complete DoS condition.			
CVE-2024-20333	Cisco	A vulnerability in the web-based management interface of Cisco Catalyst Center, formerly Cisco DNA Center, could allow an authenticated, remote attacker to change specific data within the interface on an affected device. This vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to change a specific field within the web-based management interface, even though they should not have access to change that field.	2024-03-27	4.3	Medium
CVE-2024-29240	Synology	Missing authorization vulnerability in LayoutSave webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to conduct denial-of-service attacks via unspecified vectors.	2024-03-28	4.3	Medium
CVE-2023-33855	IBM	Under certain conditions, RSA operations performed by IBM Common Cryptographic Architecture (CCA) 7.0.0 through 7.5.36 may exhibit non-constant-time behavior. This could allow a remote attacker to obtain sensitive information using a timing-based attack. IBM X-Force ID: 257676.	2024-03-26	3.7	Low