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 ٢٣ يوليو إلى ٢٩ يوليو. 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 23rd of July to 29th of July. 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-2023-34478	apache - multiple products	Apache Shiro, before 1.12.0 or 2.0.0-alpha-3, may be susceptible to a path traversal attack that results in an authentication bypass when used together with APIs or other web frameworks that route requests based on non-normalized requests. Mitigation: Update to Apache Shiro 1.12.0+ or 2.0.0-alpha-3+	2023-07-24	9.8	Critical
CVE-2023-35078	ivanti - endpoint_manager_mobile	Ivanti Endpoint Manager Mobile (EPMM), formerly MobileIron Core, through 11.10 allows remote attackers to obtain PII, add an administrative account, and change the configuration because of an authentication bypass, as exploited in the wild in July 2023. A patch is available.	2023-07-25	9.8	Critical
CVE-2023-35088	apache - inlong	Improper Neutralization of Special Elements Used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.7.0. In the toAuditCkSql method, the groupId, streamId, auditId, and dt are directly concatenated into the SQL query statement, which may lead to SQL injection attacks. Users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8198	2023-07-25	9.8	Critical
CVE-2023-37895	apache - multiple products	Java object deserialization issue in Jackrabbit webapp/standalone on all platforms allows attacker to remotely execute code via RMIVersions up to (including) 2.20.10 (stable branch) and 2.21.17 (unstable branch) use the component "commons-beanutils", which contains a class that can be used for remote code execution over RMI. Users are advised to immediately update to versions 2.20.11 or 2.21.18. Note that earlier stable branches (1.0.x .. 2.18.x) have been EOLd already and do not receive updates anymore. In general, RMI support can expose vulnerabilities by the mere presence of an exploitable class on the classpath. Even if Jackrabbit itself does not contain any code known to be exploitable anymore, adding other components to your server can expose the same type of problem. We therefore recommend to disable RMI access altogether (see further below), and will discuss deprecating RMI support in future Jackrabbit releases. How to check whether RMI support is enabledRMI support can be over an RMI-specific TCP port, and over an HTTP binding. Both are by default enabled in Jackrabbit webapp/standalone. The native RMI protocol by default uses port 1099. To check whether it is enabled, tools like "netstat" can be used to check.	2023-07-25	9.8	Critical

		RMI-over-HTTP in Jackrabbit by default uses the path "/rmi". So when running standalone on port 8080, check whether an HTTP GET request on localhost:8080/rmi returns 404 (not enabled) or 200 (enabled). Note that the HTTP path may be different when the webapp is deployed in a container as non-root context, in which case the prefix is under the user's control. Turning off RMIFind web.xml (either in JAR/WAR file or in unpacked web application folder), and remove the declaration and the mapping definition for the RemoteBindingServlet: <servlet> <servlet-name>RMI</servlet-name> <servlet-class>org.apache.jackrabbit.servlet.remote.RemoteBindingServlet</servlet-class> </servlet> <servlet-mapping> <servlet-name>RMI</servlet-name> <url-pattern>/rmi</url-pattern> </servlet-mapping> Find the bootstrap.properties file (in $REPOSITORY_HOME), and set rmi.enabled=false and also remove rmi.host rmi.port rmi.url-pattern If there is no file named bootstrap.properties in $REPOSITORY_HOME, it is located somewhere in the classpath. In this case, place a copy in $REPOSITORY_HOME and modify it as explained.			
CVE-2023-35980	arubanetworks - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-07-25	9.8	Critical
CVE-2023-35981	arubanetworks - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-07-25	9.8	Critical
CVE-2023-35982	arubanetworks - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-07-25	9.8	Critical
CVE-2023-38647	apache - helix	An attacker can use SnakeYAML to deserialize java.net.URLClassLoader and make it load a JAR from a specified URL, and then deserialize javax.script.ScriptEngineManager to load code using that ClassLoader. This unbounded deserialization can likely lead to remote code execution. The code can be run in Helix REST start and Workflow creation. Affect all the versions lower and include 1.2.0. Affected products: helix-core, helix-rest Mitigation: Short term, stop using any YAML based configuration and workflow creation. Long term, all Helix version bumping up to 1.3.0	2023-07-26	9.8	Critical
CVE-2023-33308	fortinet - multiple products	A stack-based overflow vulnerability [CWE-124] in Fortinet FortiOS version 7.0.0 through 7.0.10 and 7.2.0 through 7.2.3 and FortiProxy version 7.0.0 through 7.0.9 and 7.2.0 through 7.2.2 allows a remote unauthenticated attacker to execute arbitrary code or command via crafted packets reaching proxy policies or	2023-07-26	9.8	Critical

		firewall policies with proxy mode alongside deep or full packet inspection.			
CVE-2023-34425	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in watchOS 9.6, macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, macOS Big Sur 11.7.9, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-28	9.8	Critical
CVE-2023-36495	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in watchOS 9.6, macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-28	9.8	Critical
CVE-2023-37285	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-28	9.8	Critical
CVE-2023-38598	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.6, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-28	9.8	Critical
CVE-2023-38604	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in watchOS 9.6, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-28	9.8	Critical
CVE-2022-4920	google - chrome	Heap buffer overflow in Blink in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2023-07-29	9.6	Critical
CVE-2022-4924	google - chrome	Use after free in WebRTC in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2023-07-29	9.6	Critical
CVE-2023-2626	google - nest_hub_max_firmware	There exists an authentication bypass vulnerability in OpenThread border router devices and implementations. This issue allows unauthenticated nodes to craft radio frames using “Key ID Mode 2”: a special mode using a static encryption key to bypass security checks, resulting in arbitrary IP packets being allowed on the Thread network. This provides a pathway for an attacker to send/receive arbitrary IPv6 packets to devices on the LAN, potentially exploiting them if they lack additional authentication or contain any network vulnerabilities that would normally be mitigated by the home router’s NAT firewall. Effected devices have been mitigated through an automatic update beyond the affected range.	2023-07-25	8.8	High
CVE-2023-37450	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, Safari 16.5.2, tvOS 16.6, macOS Ventura 13.5, watchOS 9.6. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	2023-07-27	8.8	High
CVE-2023-38594	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	2023-07-27	8.8	High
CVE-2023-38597	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5, Safari 16.6. Processing web content may lead to arbitrary code execution.	2023-07-27	8.8	High
CVE-2023-32393	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in watchOS 9.3, tvOS 16.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. Processing web content may lead to arbitrary code execution.	2023-07-27	8.8	High
CVE-2023-38595	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	2023-07-27	8.8	High
CVE-2023-38600	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	2023-07-27	8.8	High
CVE-2023-38611	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	2023-07-27	8.8	High
CVE-2023-38590	apple - multiple products	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 9.6, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, tvOS 16.6,	2023-07-28	8.8	High

		iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory.			
CVE-2023-38592	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16.6 and iPadOS 16.6, watchOS 9.6, tvOS 16.6, macOS Ventura 13.5. Processing web content may lead to arbitrary code execution.	2023-07-28	8.8	High
CVE-2023-3598	google - chrome	Out of bounds read and write in ANGLE in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-07-28	8.8	High
CVE-2021-4317	google - chrome	Use after free in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2021-4318	google - chrome	Object corruption in Blink in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2021-4319	google - chrome	Use after free in Blink in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2021-4320	google - chrome	Use after free in Blink in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2021-4322	google - chrome	Use after free in DevTools in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Medium)	2023-07-29	8.8	High
CVE-2022-4906	google - chrome	Inappropriate implementation in Blink in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2022-4907	google - chrome	Uninitialized Use in FFmpeg in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	8.8	High
CVE-2022-4912	google - chrome	Type Confusion in MathML in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2022-4914	google - chrome	Heap buffer overflow in PrintPreview in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	8.8	High
CVE-2022-4916	google - chrome	Use after free in Media in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2022-4918	google - chrome	Use after free in UI in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	8.8	High
CVE-2022-4919	google - chrome	Use after free in Base Internals in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2022-4921	google - chrome	Use after free in Accessibility in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Low)	2023-07-29	8.8	High
CVE-2023-2313	google - chrome	Inappropriate implementation in Sandbox in Google Chrome on Windows prior to 112.0.5615.49 allowed a remote attacker who had compromised the renderer process to perform arbitrary read/write via a malicious file. (Chromium security severity: High)	2023-07-29	8.8	High
CVE-2023-36542	apache - nifi	Apache NiFi 0.0.2 through 1.22.0 include Processors and Controller Services that support HTTP URL references for retrieving drivers, which allows an authenticated and authorized user to configure a location that enables custom code execution. The resolution introduces a new Required Permission for referencing remote resources, restricting configuration of these components to privileged users. The permission prevents unprivileged users from configuring Processors and Controller Services annotated with the new Reference Remote Resources restriction. Upgrading to Apache NiFi 1.23.0 is the recommended mitigation.	2023-07-29	8.8	High
CVE-2023-32437	apple - multiple products	The issue was addressed with improvements to the file handling protocol. This issue is fixed in iOS 16.6 and iPadOS 16.6. An app may be able to break out of its sandbox.	2023-07-27	8.6	High
CVE-2023-32364	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.5. A sandboxed process may be able to circumvent sandbox restrictions.	2023-07-27	8.6	High

CVE-2023-32257	linux - linux_kernel	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP and SMB2_LOGOFF commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	2023-07-24	8.1	High
CVE-2023-32258	linux - linux_kernel	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_LOGOFF and SMB2_CLOSE commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	2023-07-24	8.1	High
CVE-2023-32443	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. Processing a file may lead to a denial-of-service or potentially disclose memory contents.	2023-07-27	8.1	High
CVE-2023-3640	linux - linux_kernel	A possible unauthorized memory access flaw was found in the Linux kernel's cpu_entry_area mapping of X86 CPU data to memory, where a user may guess the location of exception stacks or other important data. Based on the previous CVE-2023-0597, the 'Randomize per-cpu entry area' feature was implemented in /arch/x86/mm/cpu_entry_area.c, which works through the init_cea_offsets() function when KASLR is enabled. However, despite this feature, there is still a risk of per-cpu entry area leaks. This issue could allow a local user to gain access to some important data with memory in an expected location and potentially escalate their privileges on the system.	2023-07-24	7.8	High
CVE-2023-3812	linux - multiple products	An out-of-bounds memory access flaw was found in the Linux kernel's TUN/TAP device driver functionality in how a user generates a malicious (too big) networking packet when napi frags is enabled. This flaw allows a local user to crash or potentially escalate their privileges on the system.	2023-07-24	7.8	High
CVE-2023-32381	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.6.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-32433	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-36854	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. Processing a file may lead to unexpected app termination or arbitrary code execution.	2023-07-27	7.8	High
CVE-2023-38410	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A user may be able to elevate privileges.	2023-07-27	7.8	High
CVE-2023-32418	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. Processing a file may lead to unexpected app termination or arbitrary code execution.	2023-07-27	7.8	High
CVE-2023-32441	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-32734	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-35993	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-38136	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-38261	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-38424	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-38565	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.6.8, iOS 16.6 and iPadOS	2023-07-27	7.8	High

		16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to gain root privileges.			
CVE-2023-38580	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.8	High
CVE-2023-32450	dell - power_manager	Dell Power Manager, Versions 3.3 to 3.14 contains an Improper Access Control vulnerability. A low-privileged malicious user may potentially exploit this vulnerability to perform arbitrary code execution with limited access.	2023-07-27	7.8	High
CVE-2023-3417	mozilla - multiple products	Thunderbird allowed the Text Direction Override Unicode Character in filenames. An email attachment could be incorrectly shown as being a document file, while in fact it was an executable file. Newer versions of Thunderbird will strip the character and show the correct file extension. This vulnerability affects Thunderbird < 115.0.1 and Thunderbird < 102.13.1.	2023-07-24	7.5	High
CVE-2023-32247	linux - linux_kernel	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_SESSION_SETUP commands. The issue results from the lack of control of resource consumption. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.	2023-07-24	7.5	High
CVE-2023-32248	linux - linux_kernel	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_TREE_CONNECT and SMB2_QUERY_INFO commands. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.	2023-07-24	7.5	High
CVE-2023-32252	linux - linux_kernel	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_LOGOFF commands. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.	2023-07-24	7.5	High
CVE-2023-34434	apache - inlong	Deserialization of Untrusted Data Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.7.0. The attacker could bypass the current logic and achieve arbitrary file reading. To solve it, users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick https://github.com/apache/inlong/pull/8130 .	2023-07-25	7.5	High
CVE-2023-3442	jenkins - servicenow_devops	A missing authorization vulnerability exists in versions of the Jenkins Plug-in for ServiceNow DevOps prior to 1.38.1 that, if exploited successfully, could cause the unwanted exposure of sensitive information. To address this issue, apply the 1.38.1 version of the Jenkins plug-in for ServiceNow DevOps on your Jenkins server. No changes are required on your instances of the Now Platform.	2023-07-26	7.5	High
CVE-2023-38564	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5. An app may be able to modify protected parts of the file system.	2023-07-27	7.5	High
CVE-2023-38572	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. A website may be able to bypass Same Origin Policy.	2023-07-27	7.5	High
CVE-2023-38603	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A remote user may be able to cause a denial-of-service.	2023-07-27	7.5	High
CVE-2023-32444	apple - multiple products	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. A sandboxed process may be able to circumvent sandbox restrictions.	2023-07-28	7.5	High
CVE-2023-38571	apple - multiple products	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to bypass Privacy preferences.	2023-07-28	7.5	High
CVE-2023-38601	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to modify protected parts of the file system.	2023-07-28	7.5	High
CVE-2023-38609	apple - macos	An injection issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.5. An app may be able to bypass certain Privacy preferences.	2023-07-28	7.5	High
CVE-2023-23843	solarwinds - solarwinds_platform	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands.	2023-07-26	7.2	High

CVE-2023-23844	solarwinds - solarwinds_platform	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with SYSTEM privileges.	2023-07-26	7.2	High
CVE-2023-33224	solarwinds - solarwinds_platform	The SolarWinds Platform was susceptible to the Incorrect Behavior Order Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with NETWORK SERVICE privileges.	2023-07-26	7.2	High
CVE-2023-33225	solarwinds - solarwinds_platform	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with SYSTEM privileges.	2023-07-26	7.2	High
CVE-2023-23842	solarwinds - network_configuration_monitor	The SolarWinds Network Configuration Manager was susceptible to the Directory Traversal Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands.	2023-07-26	7.2	High
CVE-2023-38425	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-07-27	7.2	High
CVE-2023-3567	linux - multiple products	A use-after-free flaw was found in vcs_read in drivers/tty/vt/vc_screen.c in vc_screen in the Linux Kernel. This flaw allows an attacker with local user access to cause a system crash or leak internal kernel information.	2023-07-24	7.1	High
CVE-2023-33952	linux - linux_kernel	A double-free vulnerability was found in the vmwgfx driver in the Linux kernel. The flaw exists within the handling of vmw_buffer_object objects. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. This flaw allows a local privileged user to escalate privileges and execute code in the context of the kernel.	2023-07-24	6.7	Medium
CVE-2023-34189	apache - inlong	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.7.0. The attacker could use general users to delete and update the process, which only the admin can operate occurrences. Users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick https://github.com/apache/inlong/pull/8109 to solve it.	2023-07-25	6.5	Medium
CVE-2023-3637	redhat - multiple products	An uncontrolled resource consumption flaw was found in openstack-neutron. This flaw allows a remote authenticated user to query a list of security groups for an invalid project. This issue creates resources that are unconstrained by the user's quota. If a malicious user were to submit a significant number of requests, this could lead to a denial of service.	2023-07-25	6.5	Medium
CVE-2023-20891	vmware - multiple products	The VMware Tanzu Application Service for VMs and Isolation Segment contain an information disclosure vulnerability due to the logging of credentials in hex encoding in platform system audit logs. A malicious non-admin user who has access to the platform system audit logs can access hex encoded CF API admin credentials and can push new malicious versions of an application. In a default deployment non-admin users do not have access to the platform system audit logs.	2023-07-26	6.5	Medium
CVE-2023-39152	jenkins - gradle	Always-incorrect control flow implementation in Jenkins Gradle Plugin 2.8 may result in credentials not being masked (i.e., replaced with asterisks) in the build log in some circumstances.	2023-07-26	6.5	Medium
CVE-2023-39154	jenkins - qualys_web_app_scanning_connector	Incorrect permission checks in Jenkins Qualys Web App Scanning Connector Plugin 2.0.10 and earlier allow attackers with global Item/Configure permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-07-26	6.5	Medium
CVE-2023-3414	jenkins - servicenow_devops	A cross-site request forgery vulnerability exists in versions of the Jenkins Plug-in for ServiceNow DevOps prior to 1.38.1 that, if exploited successfully, could cause the unwanted exposure of sensitive information. To address this issue, apply the 1.38.1 version of the Jenkins plug-in for ServiceNow DevOps on your Jenkins server. No changes are required on your instances of the Now Platform.	2023-07-26	6.5	Medium
CVE-2023-38133	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may disclose sensitive information.	2023-07-27	6.5	Medium
CVE-2023-32654	apple - macos	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.5. A user may be able to read information belonging to another user.	2023-07-28	6.5	Medium
CVE-2023-38599	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in Safari 16.6, watchOS 9.6, iOS 15.7.8 and iPadOS 15.7.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A website may be able to track sensitive user information.	2023-07-28	6.5	Medium

CVE-2021-4323	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to access local files via a crafted Chrome Extension. (Chromium security severity: Medium)	2023-07-29	6.5	Medium
CVE-2021-4324	google - chrome	Insufficient policy enforcement in Google Update in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to read arbitrary files via a malicious file. (Chromium security severity: Medium)	2023-07-29	6.5	Medium
CVE-2022-4911	google - chrome	Insufficient data validation in DevTools in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2023-07-29	6.5	Medium
CVE-2022-4913	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who had compromised the renderer process to spoof extension storage via a crafted HTML page. (Chromium security severity: High)	2023-07-29	6.5	Medium
CVE-2022-4915	google - chrome	Inappropriate implementation in URL Formatting in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	6.5	Medium
CVE-2022-4922	google - chrome	Inappropriate implementation in Blink in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	6.5	Medium
CVE-2022-4925	google - chrome	Insufficient validation of untrusted input in QUIC in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to perform header splitting via malicious network traffic. (Chromium security severity: Low)	2023-07-29	6.5	Medium
CVE-2022-4926	google - chrome	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 109.0.5414.119 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	6.5	Medium
CVE-2023-2311	google - chrome	Insufficient policy enforcement in File System API in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	6.5	Medium
CVE-2023-2314	google - chrome	Insufficient data validation in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2023-07-29	6.5	Medium
CVE-2022-4909	google - chrome	Inappropriate implementation in XML in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially perform an ASLR bypass via a crafted HTML page. (Chromium security severity: Low)	2023-07-29	6.3	Medium
CVE-2023-38435	apache - felix_health_checks	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in Apache Felix Healthcheck Webconsole Plugin version 2.0.2 and prior may allow an attacker to perform a reflected cross-site scripting (XSS) attack. Upgrade to Apache Felix Healthcheck Webconsole Plugin 2.1.0 or higher.	2023-07-25	6.1	Medium
CVE-2023-3946	mcafee - multiple products	A reflected cross-site scripting (XSS) vulnerability in ePO prior to 5.10 SP1 Update 1allows a remote unauthenticated attacker to potentially obtain access to an ePO administrator's session by convincing the authenticated ePO administrator to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO.	2023-07-26	6.1	Medium
CVE-2023-32445	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in Safari 16.6, watchOS 9.6, iOS 15.7.8 and iPadOS 15.7.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. Processing a document may lead to a cross site scripting attack.	2023-07-28	6.1	Medium
CVE-2023-32427	apple - music	This issue was addressed by using HTTPS when sending information over the network. This issue is fixed in Apple Music 4.2.0 for Android. An attacker in a privileged network position may be able to intercept network traffic.	2023-07-28	5.9	Medium
CVE-2023-2430	linux - multiple products	A vulnerability was found due to missing lock for IOPOLL flaw in io_cqring_event_overflow() in io_uring.c in Linux Kernel. This flaw allows a local attacker with user privilege to trigger a Denial of Service threat.	2023-07-23	5.5	Medium
CVE-2023-39128	gnu - gdb	GNU gdb (GDB) 13.0.50.20220805-git was discovered to contain a stack overflow via the function ada_decode at /gdb/ada-lang.c.	2023-07-25	5.5	Medium
CVE-2023-39129	gnu - gdb	GNU gdb (GDB) 13.0.50.20220805-git was discovered to contain a heap use after free via the function add_pe_exported_sym() at /gdb/coff-pe-read.c.	2023-07-25	5.5	Medium
CVE-2023-39130	gnu - gdb	GNU gdb (GDB) 13.0.50.20220805-git was discovered to contain a heap buffer overflow via the function pe_as16() at /gdb/coff-pe-read.c.	2023-07-25	5.5	Medium

CVE-2023-35983	apple - multiple products	This issue was addressed with improved data protection. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. An app may be able to modify protected parts of the file system.	2023-07-27	5.5	Medium
CVE-2023-36862	apple - macos	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.5. An app may be able to determine a user's current location.	2023-07-27	5.5	Medium
CVE-2023-38606	apple - multiple products	This issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to modify sensitive kernel state. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.1.	2023-07-27	5.5	Medium
CVE-2023-32416	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5, watchOS 9.6. An app may be able to read sensitive location information.	2023-07-27	5.5	Medium
CVE-2023-32429	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5. An app may be able to bypass Privacy preferences.	2023-07-27	5.5	Medium
CVE-2023-32442	apple - multiple products	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Ventura 13.5, macOS Monterey 12.6.8. A shortcut may be able to modify sensitive Shortcuts app settings.	2023-07-27	5.5	Medium
CVE-2023-38258	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5, macOS Monterey 12.6.8. Processing a 3D model may result in disclosure of process memory.	2023-07-27	5.5	Medium
CVE-2023-38259	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. An app may be able to access user-sensitive data.	2023-07-27	5.5	Medium
CVE-2023-38421	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5, macOS Monterey 12.6.8. Processing a 3D model may result in disclosure of process memory.	2023-07-27	5.5	Medium
CVE-2023-38593	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.8, iOS 16.6 and iPadOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to cause a denial-of-service.	2023-07-27	5.5	Medium
CVE-2023-38602	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. An app may be able to modify protected parts of the file system.	2023-07-27	5.5	Medium
CVE-2023-38608	apple - macos	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.5. An app may be able to access user-sensitive data.	2023-07-27	5.5	Medium
CVE-2023-28203	apple - music	The issue was addressed with improved checks. This issue is fixed in Apple Music 4.2.0 for Android. An app may be able to access contacts.	2023-07-28	5.5	Medium
CVE-2023-3384	redhat - quay	A flaw was found in the Quay registry. While the image labels created through Quay undergo validation both in the UI and backend by applying a regex (validation.py), the same validation is not performed when the label comes from an image. This flaw allows an attacker to publish a malicious image to a public registry containing a script that can be executed via Cross-site scripting (XSS).	2023-07-24	5.4	Medium
CVE-2023-39151	jenkins - jenkins	Jenkins 2.415 and earlier, LTS 2.401.2 and earlier does not sanitize or properly encode URLs in build logs when transforming them into hyperlinks, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control build log contents.	2023-07-26	5.4	Medium
CVE-2023-39153	jenkins - gitlab_authentication	A cross-site request forgery (CSRF) vulnerability in Jenkins GitLab Authentication Plugin 1.17.1 and earlier allows attackers to trick users into logging in to the attacker's account.	2023-07-26	5.4	Medium
CVE-2023-38331	zohocorp - multiple products	Zoho ManageEngine Support Center Plus 14001 and below is vulnerable to stored XSS in the products module.	2023-07-28	5.4	Medium
CVE-2022-4910	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	5.4	Medium
CVE-2023-33951	linux - linux_kernel	A race condition vulnerability was found in the vmwgfx driver in the Linux kernel. The flaw exists within the handling of GEM objects. The issue results from improper locking when performing operations on an object. This flaw allows a local privileged user to disclose information in the context of the kernel.	2023-07-24	5.3	Medium
CVE-2023-3750	redhat - multiple products	A flaw was found in libvirt. The virStoragePoolObjListSearch function does not return a locked pool as expected, resulting in a race condition and denial of service when attempting to lock the	2023-07-24	5.3	Medium

		same object from another thread. This issue could allow clients connecting to the read-only socket to crash the libvirt daemon.			
CVE-2023-39155	jenkins - chef_identity	Jenkins Chef Identity Plugin 2.0.3 and earlier does not mask the user.pem key form field, increasing the potential for attackers to observe and capture it.	2023-07-26	5.3	Medium
CVE-2023-39156	jenkins - bazaar	A cross-site request forgery (CSRF) vulnerability in Jenkins Bazaar Plugin 1.22 and earlier allows attackers to delete previously created Bazaar SCM tags.	2023-07-26	5.3	Medium
CVE-2023-32468	dell - ecs_streamer	Dell ECS Streamer, versions prior to 2.0.7.1, contain an insertion of sensitive information in log files vulnerability. A remote malicious high-privileged user could potentially exploit this vulnerability leading to exposure of this sensitive data.	2023-07-26	4.9	Medium
CVE-2023-2860	linux - multiple products	An out-of-bounds read vulnerability was found in the SR-IPv6 implementation in the Linux kernel. The flaw exists within the processing of seg6 attributes. The issue results from the improper validation of user-supplied data, which can result in a read past the end of an allocated buffer. This flaw allows a privileged local user to disclose sensitive information on affected installations of the Linux kernel.	2023-07-24	4.4	Medium
CVE-2023-3772	redhat - multiple products	A flaw was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem). This issue may allow a malicious user with CAP_NET_ADMIN privileges to directly dereference a NULL pointer in xfrm_update_ae_params(), leading to a possible kernel crash and denial of service.	2023-07-25	4.4	Medium
CVE-2023-3773	redhat - multiple products	A flaw was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem). This issue may allow a malicious user with CAP_NET_ADMIN privileges to cause a 4 byte out-of-bounds read of XFRMA_MTIMER_THRESH when parsing netlink attributes, leading to potential leakage of sensitive heap data to userspace.	2023-07-25	4.4	Medium
CVE-2023-3622	solarwinds - solarwinds_platform	Access Control Bypass Vulnerability in the SolarWinds Platform that allows an underprivileged user to read arbitrary resource	2023-07-26	4.3	Medium
CVE-2021-4316	google - chrome	Inappropriate implementation in Cast UI in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to spoof browser UI via a crafted HTML page. (Chromium security severity: Low)	2023-07-29	4.3	Medium
CVE-2021-4321	google - chrome	Policy bypass in Blink in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2023-07-29	4.3	Medium
CVE-2022-4908	google - chrome	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2023-07-29	4.3	Medium
CVE-2022-4917	google - chrome	Incorrect security UI in Notifications in Google Chrome on Android prior to 103.0.5060.53 allowed a remote attacker to obscure the full screen notification via a crafted HTML page. (Chromium security severity: Low)	2023-07-29	4.3	Medium
CVE-2023-3863	linux - linux_kernel	A use-after-free flaw was found in nfc_llcp_find_local in net/nfc/llcp_core.c in NFC in the Linux kernel. This flaw allows a local user with special privileges to impact a kernel information leak issue.	2023-07-24	4.1	Medium
CVE-2023-33229	solarwinds - solarwinds_platform	The SolarWinds Platform was susceptible to the Incorrect Input Neutralization Vulnerability. This vulnerability allows a remote adversary with a valid SolarWinds Platform account to append URL parameters to inject passive HTML.	2023-07-26	3.5	Low
CVE-2022-4923	google - chrome	Inappropriate implementation in Omnibox in Google Chrome prior to 99.0.4844.51 allowed an attacker in a privileged network position to perform a man-in-the-middle attack via malicious network traffic. (Chromium security severity: Low)	2023-07-29	3.1	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.