Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

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 29th of October to 4th of November. 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**

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 ٢٩ اكتوبر إلى ٤ نوفمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـCVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-20048	cisco - multiple products	A vulnerability in the web services interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute certain unauthorized configuration commands on a Firepower Threat Defense (FTD) device that is managed by the FMC Software. This vulnerability is due to insufficient authorization of configuration commands that are sent through the web service interface. An attacker could exploit this vulnerability by authenticating to the FMC web services interface and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute certain configuration commands on the targeted FTD device. To successfully exploit this vulnerability, an attacker would need valid credentials on the FMC Software.	2023-11-01	9.9	Critical
CVE-2023-22518	atlassian - multiple products	All versions of Confluence Data Center and Server are affected by this unexploited vulnerability. This Improper Authorization vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to Confluence instance administrator leading to - but not limited to - full loss of confidentiality, integrity and availability. Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.	2023-10-31	9.8	Critical
CVE-2023-40061	solarwinds - solarwinds_platform	Insecure job execution mechanism vulnerability. This vulnerability can lead to other attacks as a result.	2023-11-01	9.8	Critical
CVE-2023-21356	google - android	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	8.8	High
CVE-2023-21361	google - android	In Bluetooth, there is a possibility of code-execution due to a use after free. This could lead to paired device escalation of privilege in the privileged Bluetooth process with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	8.8	High
CVE-2023-21392	google - android	In Bluetooth, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege when connecting to a Bluetooth device with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	8.8	High
CVE-2023-33226	solarwinds - network_configuration_manager	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows a low-level user to perform the actions with SYSTEM privileges.	2023-11-01	8.8	High
CVE-2023-33227	solarwinds - network_configuration_manager	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability This vulnerability allows a low level user to perform the actions with SYSTEM privileges.	2023-11-01	8.8	High

CVE-2023-40062	solarwinds - solarwinds_platform	SolarWinds Platform Incomplete List of Disallowed Inputs Remote Code Execution Vulnerability. If executed, this vulnerability would allow a low-privileged user to execute commands with SYSTEM privileges.	2023-11-01	8.8	High
CVE-2023-5178	linux - multiple products	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe-oF/TCP subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation in case that the attacker already has local privileges.	2023-11-01	8.8	High
CVE-2023-20219	cisco - multiple products	Multiple vulnerabilities in the web management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. The attacker would need valid device credentials but does not require administrator privileges to exploit this vulnerability. These vulnerabilities are due to insufficient validation of user-supplied input for certain configuration options. An attacker could exploit these vulnerabilities by using crafted input within the device configuration GUI. A successful exploit could allow the attacker to execute arbitrary commands on the device including the underlying operating system which could also affect the availability of the device.	2023-11-01	8.8	High
CVE-2023-20220	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. To exploit these vulnerabilities, the attacker must have valid device credentials, but does not need Administrator privileges. These vulnerabilities are due to insufficient validation of user-supplied input for certain configuration options. An attacker could exploit these vulnerabilities by using crafted input within the device configuration GUI. A successful exploit could allow the attacker to execute arbitrary commands on the device, including on the underlying operating system, which could also affect the availability of the device.	2023-11-01	8.8	High
CVE-2023-5482	google - chrome	Insufficient data validation in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2023-11-01	8.8	High
CVE-2023-5849	google - chrome	Integer overflow in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-01	8.8	High
CVE-2023-5852	google - chrome	Use after free in Printing in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	2023-11-01	8.8	High
CVE-2023-5854	google - chrome	Use after free in Profiles in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	2023-11-01	8.8	High
CVE-2023-5855	google - chrome	Use after free in Reading Mode in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	2023-11-01	8.8	High
CVE-2023-5856	google - chrome	Use after free in Side Panel in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-11-01	8.8	High
CVE-2023-5857	google - chrome	Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially execute arbitrary code via a malicious file. (Chromium security severity: Medium)	2023-11-01	8.8	High
CVE-2023-42027	ibm - multiple products	IBM CICS TX Standard 11.1, Advanced 10.1, 11.1, and TXSeries for Multiplatforms 8.1, 8.2, 9.1 are 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: 266057.	2023-11-03	8.8	High
CVE-2023-20063	cisco - multiple products	A vulnerability in the inter-device communication mechanisms between devices that are running Cisco Firepower Threat Defense (FTD) Software and devices that are running Cisco Firepower Management (FMC) Software could allow an authenticated, local attacker to execute arbitrary commands with root permissions on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by accessing the expert mode of an affected device and submitting specific commands to a connected system. A successful exploit could allow the attacker to	2023-11-01	8.2	High

		execute arbitrary code in the context of an FMC device if the attacker has administrative privileges on an associated FTD device. Alternatively, a successful exploit could allow the attacker to execute arbitrary code in the context of an FTD device if the attacker has administrative privileges on an associated FMC device.			
CVE-2023-40686	ibm - multiple products	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain component access to the operating system. IBM X-Force ID: 264114.	2023-10-29	7.8	High
CVE-2023-40685	ibm - multiple products	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain root access to the operating system. IBM X-Force ID: 264116.	2023-10-29	7.8	High
CVE-2021-39810	google - multiple products	In NFC, there is a possible way to setup a default contactless payment app without user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21298	google - android	In Slice, there is a possible disclosure of installed applications due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21313	google - android	In Core, there is a possible way to forward calls without user knowledge due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21324	google - android	In Package Installer, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21328	google - android	In Package Installer, there is a possible way to determine whether an app is installed, without query permissions, due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21337	google - android	In InputMethod, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21341	google - android	In Permission Manager, there is a possible way to bypass required permissions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21342	google - android	In Speech, there is a possible way to bypass background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21343	google - android	In ActivityStarter, there is a possible background activity launch due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21351	google - android	In Activity Manager, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21355	google - android	In libaudioclient, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21358	google - android	In UWB Google, there is a possible way for a malicious app to masquerade as system app com.android.uwb.resources due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21372	google - android	In libdexfile, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21373	google - android	In Telephony, there is a possible way for a guest user to change the preferred SIM due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21374	google - android	In System UI, there is a possible factory reset protection bypass due to a logic error in the code. This could lead to local escalation of	2023-10-30	7.8	High

		privilege with no additional execution privileges needed. User interaction is not needed for exploitation.			
CVE-2023-21375	google - android	In Sysproxy, there is a possible out of bounds write due to an integer underflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21378	google - android	In Telecomm, there is a possible way to silence the ring for calls of secondary users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21381	google - android	In Media Resource Manager, there is a possible local arbitrary code execution due to use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21388	google - android	In Settings, there is a possible restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21389	google - android	In Settings, there is a possible bypass of profile owner restrictions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21390	google - android	In Sim, there is a possible way to evade mobile preference restrictions due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21393	google - android	In Settings, there is a possible way for the user to change SIM due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21396	google - android	In Activity Manager, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21397	google - android	In Setup Wizard, there is a possible way to save a WiFi network due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-21398	google - android	In sdksandbox, there is a possible strandhogg style overlay attack due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.8	High
CVE-2023-5739	hp - multiple products	Certain versions of HP PC Hardware Diagnostics Windows are potentially vulnerable to elevation of privilege.	2023-10-31	7.8	High
CVE-2023-3972	redhat - insights-client	A vulnerability was found in insights-client. This security issue occurs because of insecure file operations or unsafe handling of temporary files and directories that lead to local privilege escalation. Before the insights-client has been registered on the system by root, an unprivileged local user or attacker could create the /var/tmp/insights-client directory (owning the directory with read, write, and execute permissions) on the system. After the insights-client is registered by root, an attacker could then control the directory content that insights are using by putting malicious scripts into it and executing arbitrary code as root (trivially bypassing SELinux protections because insights processes are allowed to disable SELinux system-wide).	2023-11-01	7.8	High
CVE-2023-20175	cisco - multiple products	A vulnerability in a specific Cisco ISE CLI command could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, an attacker must have valid Read-only-level privileges or higher on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-11-01	7.8	High
CVE-2023-46176	ibm - mq_appliance	IBM MQ Appliance 9.3 CD could allow a local attacker to gain elevated privileges on the system, caused by improper validation of security keys. IBM X-Force ID: 269535.	2023-11-03	7.8	High
CVE-2022-43554	ivanti - avalanche	Ivanti Avalanche Smart Device Service Missing Authentication Local Privilege Escalation Vulnerability	2023-11-03	7.8	High
CVE-2022-43555	ivanti - avalanche	Ivanti Avalanche Printer Device Service Missing Authentication Local Privilege Escalation Vulnerability	2023-11-03	7.8	High
CVE-2022-44569	ivanti - automation	A locally authenticated attacker with low privileges can bypass authentication due to insecure inter-process communication.	2023-11-03	7.8	High
CVE-2023-41725	ivanti - avalanche	Ivanti Avalanche EnterpriseServer Service Unrestricted File Upload Local Privilege Escalation Vulnerability	2023-11-03	7.8	High
CVE-2023-41726	ivanti - avalanche	Ivanti Avalanche Incorrect Default Permissions allows Local Privilege Escalation Vulnerability	2023-11-03	7.8	High

CVE-2023-21339	google - android	In Minikin, there is a possible way to trigger ANR by showing a malicious message due to resource exhaustion. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.5	High
CVE-2023-21347	google - android	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.5	High
CVE-2023-21353	google - android	In NFA, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.5	High
CVE-2023-21391	google - android	In Messaging, there is a possible way to disable the messaging application due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	7.5	High
CVE-2023-5625	redhat - multiple products	A regression was introduced in the Red Hat build of python-eventlet due to a change in the patch application strategy, resulting in a patch for CVE-2021-21419 not being applied for all builds of all products.	2023-11-01	7.5	High
CVE-2023-20086	cisco - multiple products	A vulnerability in ICMPv6 processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper processing of ICMPv6 messages. An attacker could exploit this vulnerability by sending crafted ICMPv6 messages to a targeted Cisco ASA or FTD system with IPv6 enabled. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	2023-11-01	7.5	High
CVE-2023-20083	cisco - multiple products	A vulnerability in ICMPv6 inspection when configured with the Snort 2 detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the CPU of an affected device to spike to 100 percent, which could stop all traffic processing and result in a denial of service (DoS) condition. FTD management traffic is not affected by this vulnerability. This vulnerability is due to improper error checking when parsing fields within the ICMPv6 header. An attacker could exploit this vulnerability by sending a crafted ICMPv6 packet through 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. Note: To recover from the DoS condition, the Snort 2 Detection Engine or the Cisco FTD device may need to be restarted.	2023-11-01	7.5	High
CVE-2023-20095	cisco - multiple products	A vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of HTTPS requests. An attacker could exploit this vulnerability by sending crafted HTTPS requests to an affected system. A successful exploit could allow the attacker to cause resource exhaustion, resulting in a DoS condition.	2023-11-01	7.5	High
CVE-2023-43018	ibm - multiple products	IBM CICS TX Standard 11.1 and Advanced 10.1, 11.1 performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 266163.	2023-11-03	7.5	High
CVE-2023-45780	google - android	In Print Service, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2023-10-30	7.3	High
CVE-2023-20196	cisco - multiple products	Two vulnerabilities in Cisco ISE could allow an authenticated, remote attacker to upload arbitrary files to an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. These vulnerabilities are due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit these vulnerabilities by uploading a crafted file to an affected device. A successful exploit could allow the attacker to store malicious files in specific directories on the device. The attacker could later use those files to conduct additional attacks, including executing arbitrary code on the affected device with root privileges.	2023-11-01	7.2	High
CVE-2023-5408	redhat - openshift_container_platform	A privilege escalation flaw was found in the node restriction admission plugin of the kubernetes api server of OpenShift. A remote attacker who modifies the node role label could steer workloads from the control plane and etcd nodes onto different worker nodes and gain broader access to the cluster.	2023-11-02	7.2	High

CVE-2022-48189	lenovo - thinkpad_e14_firmware	An SMM driver input validation vulnerability in the BIOS of some ThinkPad models could allow an attacker with local access and elevated privileges to execute arbitrary code.	2023-10-30	6.7	Medium
CVE-2022-4573	lenovo - thinkpad_x1_fold_gen_1_firmware	An SMI handler input validation vulnerability in the ThinkPad X1 Fold Gen 1 could allow an attacker with local access and elevated privileges to execute arbitrary code.	2023-10-30	6.7	Medium
CVE-2022-4574	lenovo - thinkpad_x13_yoga_gen_2_firmware	An SMI handler input validation vulnerability in the BIOS of some ThinkPad models could allow an attacker with local access and elevated privileges to execute arbitrary code.	2023-10-30	6.7	Medium
CVE-2022-4575	lenovo - thinkpad_25_firmware	A vulnerability due to improper write protection of UEFI variables was reported in the BIOS of some ThinkPad models could allow an attacker with physical or local access and elevated privileges the ability to bypass Secure Boot.	2023-10-30	6.7	Medium
CVE-2023-21310	google - android	In Bluetooth, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	6.7	Medium
CVE-2023-21360	google - android	In Bluetooth, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	6.7	Medium
CVE-2023-21370	google - android	In the Security Element API, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	6.7	Medium
CVE-2023-21371	google - android	In Secure Element, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	6.7	Medium
CVE-2023-21380	google - android	In Bluetooth, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	6.7	Medium
CVE-2023-42655	google - android	In sim service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed	2023-11-01	6.7	Medium
CVE-2023-20170	cisco - multiple products	A vulnerability in a specific Cisco ISE CLI command could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, an attacker must have valid Administrator-level privileges on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-11-01	6.7	Medium
CVE-2023-21315	google - android	In Bluetooth, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote (proximal/adjacent) information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	6.5	Medium
CVE-2023-21395	google - android	In Bluetooth, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	6.5	Medium
CVE-2023-39610	tp-link - tapo_c100_firmware	An issue in TP-Link Tapo C100 v1.1.15 Build 211130 Rel.15378n(4555) and before allows attackers to cause a Denial of Service (DoS) via supplying a crafted web request.	2023-10-31	6.5	Medium
CVE-2023-20114	cisco - multiple products	A vulnerability in the file download feature of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to download arbitrary files from an affected system. This vulnerability is due to a lack of input sanitation. An attacker could exploit this vulnerability by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from the affected system.	2023-11-01	6.5	Medium
CVE-2023-20155	cisco - multiple products	A vulnerability in a logging API in Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to cause the device to become unresponsive or trigger an unexpected reload. This vulnerability could also allow an attacker with valid user credentials, but not Administrator privileges, to view a system log file that they would not normally have access to. This vulnerability is due to a lack of rate-limiting of requests that are sent to a specific API that is related to an FMC log. An attacker could exploit this vulnerability by sending a high rate of HTTP requests to the API. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the FMC CPU spiking to 100 percent utilization or to the device reloading. CPU utilization would return to normal if the attack traffic was stopped before an unexpected reload was triggered.	2023-11-01	6.5	Medium

CVE-2023-1192	linux - linux_kernel	A use-after-free flaw was found in smb2_is_status_io_timeout() in CIFS in the Linux Kernel. After CIFS transfers response data to a system call, there are still local variable points to the memory region, and if the system call frees it faster than CIFS uses it, CIFS will access a free memory region, leading to a denial of service.	2023-11-01	6.5	Medium
CVE-2023-1193	linux - multiple products	A use-after-free flaw was found in setup_async_work in the KSMBD implementation of the in-kernel samba server and CIFS in the Linux kernel. This issue could allow an attacker to crash the system by accessing freed work.	2023-11-01	6.5	Medium
CVE-2023-43076	dell - multiple products	Dell PowerScale OneFS 8.2.x,9.0.0.x-9.5.0.x contains a denial-of-service vulnerability. A low privilege remote attacker could potentially exploit this vulnerability to cause an out of memory (OOM) condition.	2023-11-02	6.5	Medium
CVE-2023-43087	dell - multiple products	Dell PowerScale OneFS 8.2.x, 9.0.0.x-9.5.0.x contains an improper handling of insufficient permissions. A low privileged remote attacker could potentially exploit this vulnerability to cause information disclosure.	2023-11-02	6.5	Medium
CVE-2023-45189	ibm - multiple products	A vulnerability in IBM Robotic Process Automation and IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.10, 23.0.0 through 23.0.10 may result in access to client vault credentials. This difficult to exploit vulnerability could allow a low privileged attacker to programmatically access client vault credentials. IBM X-Force ID: 268752.	2023-11-03	6.5	Medium
CVE-2023-3397	linux - linux_kernel	A race condition occurred between the functions lmLogClose and txEnd in JFS, in the Linux Kernel, executed in different threads. This flaw allows a local attacker with normal user privileges to crash the system or leak internal kernel information.	2023-11-01	6.3	Medium
CVE-2023-4964	microfocus - multiple products	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites.	2023-10-30	6.1	Medium
CVE-2023-36920	sap - multiple products	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-FRAME-OPTIONS response header is not implemented, allowing an unauthenticated attacker to attempt clickjacking, which could result in disclosure or modification of information.	2023-10-30	6.1	Medium
CVE-2023-20886	vmware - multiple products	VMware Workspace ONE UEM console contains an open redirect vulnerability. A malicious actor may be able to redirect a victim to an attacker and retrieve their SAML response to login as the victim user.	2023-10-31	6.1	Medium
CVE-2023-20005	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	2023-11-01	6.1	Medium
CVE-2023-20041	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	2023-11-01	6.1	Medium
CVE-2023-20074	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful	2023-11-01	6.1	Medium

		exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.			
CVE-2023-20206	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	2023-11-01	6.1	Medium
CVE-2023-5480	google - chrome	Inappropriate implementation in Payments in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to bypass XSS preventions via a malicious file. (Chromium security severity: High)	2023-11-01	6.1	Medium
CVE-2023-20071	cisco - multiple products	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. This vulnerability is due to a flaw in the FTP module of the Snort detection engine. An attacker could exploit this vulnerability by sending crafted FTP traffic through an affected device. A successful exploit could allow the attacker to bypass FTP inspection and deliver a malicious payload.	2023-11-01	5.8	Medium
CVE-2023-44323	microsoft - edge_chromium	Adobe Acrobat for Edge version 118.0.2088.46 (and earlier) is affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-10-30	5.5	Medium
CVE-2022-20264	google - android	In Usage Stats Service, there is a possible way to determine whether an app is installed, without query permissions due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21293	google - android	In PackageManagerNative, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21294	google - android	In Slice, there is a possible disclosure of installed packages due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21295	google - android	In SliceManagerService, there is a possible way to check if a content provider is installed due to a missing null check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21296	google - android	In Permission, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21299	google - android	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21300	google - android	In PackageManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21301	google - android	In ActivityManagerService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21302	google - android	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21303	google - android	In Content, here is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information	2023-10-30	5.5	Medium

		disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.			
CVE-2023-21304	google - android	In Content Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21305	google - android	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21306	google - android	In ContentService, there is a possible way to read installed sync content providers due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21308	google - android	In Composer, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21309	google - android	In libcore, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21311	google - android	In Settings, there is a possible way to control private DNS settings from a secondary user due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21312	google - android	In IntentResolver, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21316	google - android	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21317	google - android	In ContentService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21318	google - android	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21319	google - android	In UsageStatsService, there is a possible way to read installed 3rd party apps due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21320	google - android	In Device Policy, there is a possible way to verify if a particular admin app is registered on the device due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21321	google - android	In Package Manager, there is a possible cross-user settings disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21323	google - android	In Activity Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21325	google - android	In Settings, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21326	google - android	In Package Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21327	google - android	In Permission Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information	2023-10-30	5.5	Medium

		disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.			
CVE-2023-21329	google - android	In Activity Manager, there is a possible way to determine whether an app is installed due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21330	google - android	In Overlay Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21331	google - android	In InputMethod, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21332	google - android	In Text Services, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21333	google - android	In Text Services, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21334	google - android	In App Ops Service, there is a possible disclosure of information about installed packages due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21335	google - android	In Settings, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21336	google - android	In Input Method, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21338	google - android	In Input Method, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21340	google - android	In Telecomm, there is a possible way to get the call state due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21344	google - android	In Job Scheduler, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21350	google - android	In Media Projection, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21352	google - android	In NFA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21354	google - android	In Package Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21362	google - android	In Usage, there is a possible permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21364	google - multiple products	In ContactsProvider, there is a possible crash loop due to resource exhaustion. This could lead to local persistent denial of service in the Phone app with User execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21365	google - android	In Contacts, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service in the Phone	2023-10-30	5.5	Medium

		app with User execution privileges needed. User interaction is not needed for exploitation.			
CVE-2023-21366	google - multiple products	In Scudo, there is a possible way for an attacker to predict heap allocation patterns due to insecure implementation/design. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21367	google - android	In Scudo, there is a possible way to exploit certain heap OOB read/write issues due to an insecure implementation/design. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21368	google - android	In Audio, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21369	google - android	In Usage Access, there is a possible way to display a Settings usage access restriction toggle screen due to a permissions bypass. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21376	google - android	In Telephony, there is a possible way to retrieve the ICCID due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21377	google - android	In SELinux Policy, there is a possible restriction bypass due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21382	google - android	In Content Resolver, there is a possible method to access metadata about existing content providers on the device due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21383	google - android	In Settings, there is a possible way for the user to unintentionally send extra data due to an unclear prompt. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21384	google - android	In Package Manager, there is a possible possible permissions bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21385	google - android	In Whitechapel, there is a possible out of bounds read due to memory corruption. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-21394	google - android	In Telecomm, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2023-40101	google - android	In collapse of canonicalize_md.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	5.5	Medium
CVE-2022-48454	google - multiple products	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2022-48455	google - multiple products	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2022-48457	google - multiple products	In TeleService, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2022-48458	google - multiple products	In TeleService, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2022-48459	google - multiple products	In TeleService, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2022-48460	google - multiple products	In setting service, there is a possible undefined behavior due to incorrect error handling. This could lead to local denial of service with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42631	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42632	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium

CVE-2023-42633	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42634	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42635	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42636	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42637	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42638	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42639	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42640	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42641	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42642	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42643	google - multiple products	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42644	google - multiple products	In dm service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42645	google - android	In sim service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42646	google - multiple products	In Ifaa service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42647	google - multiple products	In Ifaa service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42648	google - multiple products	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42649	google - multiple products	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42650	google - multiple products	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42651	google - multiple products	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42652	google - multiple products	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2023-42653	google - multiple products	In faceid service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges	2023-11-01	5.5	Medium
CVE-2023-42654	google - multiple products	In dm service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-11-01	5.5	Medium
CVE-2022-4900	php - php	A vulnerability was found in PHP where setting the environment variable PHP_CLI_SERVER_WORKERS to a large value leads to a heap buffer overflow.	2023-11-02	5.5	Medium
CVE-2023-42029	ibm - multiple products	IBM CICS TX Standard 11.1, Advanced 10.1, 11.1, and TXSeries for Multiplatforms 8.1, 8.2, 9.1 are 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: 266059.	2023-11-03	5.4	Medium
CVE-2023-35896	ibm - content_navigator	IBM Content Navigator 3.0.13 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send	2023-11-03	5.4	Medium

		unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 259247.			
CVE-2023-20255	cisco - meeting_server	A vulnerability in an API of the Web Bridge feature of Cisco Meeting Server could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP packets to an affected device. A successful exploit could allow the attacker to cause a partial availability condition, which could cause ongoing video calls to be dropped due to the invalid packets reaching the Web Bridge.	2023-11-01	5.3	Medium
CVE-2023-20267	cisco - firepower_threat_defense	A vulnerability in the IP geolocation rules of Snort 3 could allow an unauthenticated, remote attacker to potentially bypass IP address restrictions. This vulnerability exists because the configuration for IP geolocation rules is not parsed properly. An attacker could exploit this vulnerability by spoofing an IP address until they bypass the restriction. A successful exploit could allow the attacker to bypass location-based IP address restrictions.	2023-11-01	5.3	Medium
CVE-2023-21307	google - android	In Bluetooth, there is a possible way for a paired Bluetooth device to access a long term identifier for an Android device due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2023-10-30	5	Medium
CVE-2023-43041	ibm - multiple products	IBM QRadar SIEM 7.5 is vulnerable to information exposure allowing a delegated Admin tenant user with a specific domain security profile assigned to see data from other domains. This vulnerability is due to an incomplete fix for CVE-2022-34352. IBM X-Force ID: 266808.	2023-10-29	4.9	Medium
CVE-2023-33228	solarwinds - network_configuration_manager	The SolarWinds Network Configuration Manager was susceptible to the Exposure of Sensitive Information Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to obtain sensitive information.	2023-11-01	4.9	Medium
CVE-2023-46862	linux - linux_kernel	An issue was discovered in the Linux kernel through 6.5.9. During a race with SQ thread exit, an io_uring/fdinfo.c io_uring_show_fdinfo NULL pointer dereference can occur.	2023-10-29	4.7	Medium
CVE-2023-21297	google - android	In SEPolicy, there is a possible way to access the factory MAC address due to a permissions bypass. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	4.4	Medium
CVE-2023-21314	google - android	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	4.4	Medium
CVE-2023-21357	google - android	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	4.4	Medium
CVE-2023-21359	google - android	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	4.4	Medium
CVE-2023-21379	google - android	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	4.4	Medium
CVE-2023-21387	google - android	In User Backup Manager, there is a possible way to leak a token to bypass user confirmation for backup due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	4.4	Medium
CVE-2022-48456	google - multiple products	In camera driver, there is a possible out of bounds write due to a incorrect bounds check. This could lead to local denial of service with System execution privileges needed	2023-11-01	4.4	Medium
CVE-2022-48461	google - multiple products	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-11-01	4.4	Medium
CVE-2023-42750	google - multiple products	In gnss service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-11-01	4.4	Medium
CVE-2023-20247	cisco - multiple products	A vulnerability in the remote access SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to bypass a configured multiple certificate authentication policy and connect using only a valid username and password. This vulnerability is due to improper error handling during remote access VPN authentication. An attacker could exploit this vulnerability by sending crafted requests during remote access VPN session establishment. A successful exploit could allow the attacker to bypass the configured multiple certificate	2023-11-01	4.3	Medium

		authentication policy while retaining the privileges and permissions associated with the original connection profile.			
CVE-2023-5850	google - chrome	Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium)	2023-11-01	4.3	Medium
CVE-2023-5851	google - chrome	Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-11-01	4.3	Medium
CVE-2023-5853	google - chrome	Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-11-01	4.3	Medium
CVE-2023-5858	google - chrome	Inappropriate implementation in WebApp Provider in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Low)	2023-11-01	4.3	Medium
CVE-2023-5859	google - chrome	Incorrect security UI in Picture In Picture in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform domain spoofing via a crafted local HTML page. (Chromium security severity: Low)	2023-11-01	4.3	Medium
CVE-2023-21345	google - android	In Game Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	3.3	Low
CVE-2023-21346	google - android	In the Device Idle Controller, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	3.3	Low
CVE-2023-21348	google - android	In Window Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	3.3	Low
CVE-2023-21349	google - android	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-30	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.