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 ١٢ ماي إلى ١٨ ماي. 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

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 12th of May to 18th of May. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-29895	Cacti	Cacti provides an operational monitoring and fault management framework. A command injection vulnerability on the 1.3.x DEV branch allows any unauthenticated user to execute arbitrary command on the server when `register_argc_argv` option of PHP is `On`. In `cmd_realtime.php` line 119, the `$poller_id` used as part of the command execution is sourced from `$_SERVER['argv']`, which can be controlled by URL when `register_argc_argv` option of PHP is `On`. And this option is `On` by default in many environments such as the main PHP Docker image for PHP. Commit 53e8014d1f082034e0646edc6286cde3800c683d contains a patch for the issue, but this commit was reverted in commit 99633903cad0de5ace636249de16f77e57a3c8fc.	2024-05-14	10	Critical
CVE-2024-30207	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The affected systems use symmetric cryptography with a hard-coded key to protect the communication between client and server. This could allow an unauthenticated remote attacker to compromise confidentiality and integrity of the communication and, subsequently, availability of the system. A successful exploit requires the attacker to gain knowledge of the hard-coded key and to be able to intercept the communication between client and server on the network.	2024-05-14	10	Critical
CVE-2024-32741	Siemens	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V3.0). The affected device contains hard coded password which is used for the privileged system user `root` and for the boot loader `GRUB` by default . An attacker who manages to crack the password hash gains root access to the device.	2024-05-14	10	Critical
CVE-2024-29212	Veeam	Due to an unsafe de-serialization method used by the Veeam Service Provider Console(VSPC) server in communication between the management agent and its components, under certain conditions, it is possible to perform Remote Code Execution (RCE) on the VSPC server machine.	2024-05-14	9.9	Critical
CVE-2024-27939	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow the upload of arbitrary files of any unauthenticated user. An attacker could leverage this vulnerability and achieve arbitrary code execution with system privileges.	2024-05-14	9.8	Critical
CVE-2024-32740	Siemens	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V3.0). The affected device contains undocumented users and credentials. An attacker could misuse the credentials to	2024-05-14	9.8	Critical

		compromise the device locally or over the network.			
CVE-2024-4671	Google	Use after free in Visuals in Google Chrome prior to 124.0.6367.201 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)	2024-05-14	9.6	Critical
CVE-2024-30209	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected systems transmit client-side resources without proper cryptographic protection. This could allow an attacker to eavesdrop on and modify resources in transit. A successful exploit requires an attacker to be in the network path between the RTLS Locating Manager server and a client (MitM).	2024-05-14	9.6	Critical
CVE-2023-47709	IBM	IBM Security Guardium 11.3, 11.4, 11.5, and 12.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 271524.	2024-05-14	9.1	Critical
CVE-2024-25641	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, an arbitrary file write vulnerability, exploitable through the "Package Import" feature, allows authenticated users having the "Import Templates" permission to execute arbitrary PHP code on the web server. The vulnerability is located within the `import_package()` function defined into the `/lib/import.php` script. The function blindly trusts the filename and file content provided within the XML data, and writes such files into the Cacti base path (or even outside, since path traversal sequences are not filtered). This can be exploited to write or overwrite arbitrary files on the web server, leading to execution of arbitrary PHP code or other security impacts. Version 1.2.27 contains a patch for this issue.	2024-05-14	9.1	Critical
CVE-2024-34340	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, Cacti calls `compat_password_hash` when users set their password. `compat_password_hash` use `password_hash` if there is it, else use `md5`. When verifying password, it calls `compat_password_verify`. In `compat_password_verify`, `password_verify` is called if there is it, else use `md5`. `password_verify` and `password_hash` are supported on PHP < 5.5.0, following PHP manual. The vulnerability is in `compat_password_verify`. Md5-hashed user input is compared with correct password in database by `$md5 == $hash`. It is a loose comparison, not `===`. It is a type juggling vulnerability. Version 1.2.27 contains a patch for the issue.	2024-05-14	9.1	Critical
CVE-2024-33499	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The affected application assigns incorrect permissions to a user management component. This could allow a privileged attacker to escalate their privileges from the Administrators group to the Systemadministrator group.	2024-05-14	9.1	Critical
CVE-2024-28075	SolarWinds	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	2024-05-14	9	Critical
CVE-2024-31445	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, a SQL injection vulnerability in `automation_get_new_graphs_sql` function of `api_automation.php` allows authenticated users to exploit these SQL injection vulnerabilities to perform privilege escalation and remote code execution. In `api_automation.php` line 856, the `get_request_var('filter')` is being concatenated into the SQL statement without any sanitization. In `api_automation.php` line	2024-05-14	8.8	High

		717, The filter of `'filter'` is `FILTER_DEFAULT`, which means there is no filter for it. Version 1.2.27 contains a patch for the issue.			
CVE-2024-27940	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow any authenticated user to send arbitrary SQL commands to the SQL server. An attacker could use this vulnerability to compromise the whole database.	2024-05-14	8.8	High
CVE-2024-27941	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected client systems do not properly sanitize input data before sending it to the SQL server. An attacker could use this vulnerability to compromise the whole database.	2024-05-14	8.8	High
CVE-2024-30206	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected SIMATIC RTLS Locating Manager Clients do not properly check the integrity of update files. This could allow an unauthenticated remote attacker to alter update files in transit and trick an authorized user into installing malicious code. A successful exploit requires the attacker to be able to modify the communication between server and client on the network.	2024-05-14	8.8	High
CVE-2024-4761	Google	Out of bounds write in V8 in Google Chrome prior to 124.0.6367.207 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2024-05-14	8.8	High
CVE-2024-30006	Microsoft	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-05-14	8.8	High
CVE-2024-30007	Microsoft	Microsoft Brokering File System Elevation of Privilege Vulnerability	2024-05-14	8.8	High
CVE-2024-30009	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-05-14	8.8	High
CVE-2024-30010	Microsoft	Windows Hyper-V Remote Code Execution Vulnerability	2024-05-14	8.8	High
CVE-2024-30017	Microsoft	Windows Hyper-V Remote Code Execution Vulnerability	2024-05-14	8.8	High
CVE-2024-30040	Microsoft	Windows MSHTML Platform Security Feature Bypass Vulnerability	2024-05-14	8.8	High
CVE-2024-31491	Fortinet	A client-side enforcement of server-side security in Fortinet FortiSandbox version 4.4.0 through 4.4.4 and 4.2.0 through 4.2.6 allows attacker to execute unauthorized code or commands via HTTP requests.	2024-05-14	8.8	High
CVE-2024-23473	SolarWinds	The SolarWinds Access Rights Manager was found to contain a hard-coded credential authentication bypass vulnerability. If exploited, this vulnerability allows access to the RabbitMQ management console. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	2024-05-14	8.6	High
CVE-2024-32997	Huawei	Race condition vulnerability in the binder driver module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	8.4	High
CVE-2024-30020	Microsoft	Windows Cryptographic Services Remote Code Execution Vulnerability	2024-05-14	8.1	High
CVE-2024-31459	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, there is a file inclusion issue in the `lib/plugin.php` file. Combined with SQL injection vulnerabilities, remote code execution can be implemented. There is a file inclusion issue with the `api_plugin_hook()` function in the `lib/plugin.php` file, which reads the plugin_hooks and plugin_config tables in database. The read data is directly used to concatenate the file path which is used for file inclusion. Version 1.2.27 contains a patch for the issue.	2024-05-14	8	High
CVE-2023-47712	IBM	IBM Security Guardium 11.3, 11.4, 11.5, and 12.0 could allow a local user to gain elevated privileges on the system due to improper permissions control. IBM X-Force ID: 271527.	2024-05-14	7.8	High
CVE-2024-31484	Siemens	A vulnerability has been identified in CPC80 Central Processing/Communication (All versions < V16.41), CPCI85 Central Processing/Communication (All versions < V5.30). The affected device firmwares contain an improper null termination vulnerability while parsing a specific HTTP header. This could allow an attacker to execute code in the context of the current process or lead to denial of service condition.	2024-05-14	7.8	High
CVE-2024-31980	Siemens	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.256), Parasolid V36.0 (All versions < V36.0.210), Parasolid V36.1 (All versions < V36.1.185). The affected application contains an out of bounds write past the end of an allocated buffer while	2024-05-14	7.8	High

		parsing a specially crafted X_T part file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-23468)			
CVE-2024-32055	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-32057	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21562)	2024-05-14	7.8	High
CVE-2024-32058	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected application is vulnerable to memory corruption while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21563)	2024-05-14	7.8	High
CVE-2024-32059	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21564)	2024-05-14	7.8	High
CVE-2024-32060	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21565)	2024-05-14	7.8	High
CVE-2024-32061	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21566)	2024-05-14	7.8	High
CVE-2024-32062	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21568)	2024-05-14	7.8	High
CVE-2024-32063	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21573)	2024-05-14	7.8	High
CVE-2024-32064	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21575)	2024-05-14	7.8	High
CVE-2024-32065	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21577)	2024-05-14	7.8	High
CVE-2024-32066	Siemens	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V27.1.215). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21578)	2024-05-14	7.8	High
CVE-2024-32635	Siemens	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.256), Parasolid V36.0 (All versions < V36.0.208), Parasolid V36.1 (All versions < V36.1.173). The affected applications contain an out of bounds read past the unmapped memory region while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-32636	Siemens	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.256), Parasolid V36.0 (All versions < V36.0.208), Parasolid V36.1 (All versions < V36.1.173). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-32639	Siemens	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0011). The affected application contains an out of bounds write past the end of an allocated buffer	2024-05-14	7.8	High

		while parsing a specially crafted MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22974)			
CVE-2024-33489	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-33490	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-33491	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-33492	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-33493	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-33577	Siemens	A vulnerability has been identified in Simcenter Nastran 2306 (All versions), Simcenter Nastran 2312 (All versions), Simcenter Nastran 2406 (All versions < V2406.90). The affected applications contain a stack overflow vulnerability while parsing specially strings as argument for one of the application binaries. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-34085	Siemens	A vulnerability has been identified in JT2Go (All versions < V2312.0001), Teamcenter Visualization V14.1 (All versions < V14.1.0.13), Teamcenter Visualization V14.2 (All versions < V14.2.0.10), Teamcenter Visualization V14.3 (All versions < V14.3.0.7), Teamcenter Visualization V2312 (All versions < V2312.0001). The affected applications contain a stack overflow vulnerability while parsing specially crafted XML files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-34086	Siemens	A vulnerability has been identified in JT2Go (All versions < V2312.0001), Teamcenter Visualization V14.1 (All versions < V14.1.0.13), Teamcenter Visualization V14.2 (All versions < V14.2.0.10), Teamcenter Visualization V14.3 (All versions < V14.3.0.7), Teamcenter Visualization V2312 (All versions < V2312.0001). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted CGM file. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-34771	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 2). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-34772	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 4). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-34773	Siemens	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 2). The affected applications contain a stack overflow vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-05-14	7.8	High
CVE-2024-26238	Microsoft	Microsoft PLUGScheduler Scheduled Task Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-29994	Microsoft	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-29996	Microsoft	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30018	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30025	Microsoft	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30027	Microsoft	NTFS Elevation of Privilege Vulnerability	2024-05-14	7.8	High

CVE-2024-30028	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30030	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30031	Microsoft	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30032	Microsoft	Windows DWM Core Library Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30035	Microsoft	Windows DWM Core Library Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30038	Microsoft	Win32k Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30042	Microsoft	Microsoft Excel Remote Code Execution Vulnerability	2024-05-14	7.8	High
CVE-2024-30049	Microsoft	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-30051	Microsoft	Windows DWM Core Library Elevation of Privilege Vulnerability	2024-05-14	7.8	High
CVE-2024-27082	Cacti	Cacti provides an operational monitoring and fault management framework. Versions of Cacti prior to 1.2.27 are vulnerable to stored cross-site scripting, a type of cross-site scripting where malicious scripts are permanently stored on a target server and served to users who access a particular page. Version 1.2.27 contains a patch for the issue.	2024-05-14	7.6	High
CVE-2024-32742	Siemens	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V3.0). The affected device contains an unrestricted USB port. An attacker with local access to the device could potentially misuse the port for booting another operating system and gain complete read/write access to the filesystem.	2024-05-14	7.6	High
CVE-2024-30047	Microsoft	Dynamics 365 Customer Insights Spoofing Vulnerability	2024-05-14	7.6	High
CVE-2024-30048	Microsoft	Dynamics 365 Customer Insights Spoofing Vulnerability	2024-05-14	7.6	High
CVE-2024-32991	Huawei	Permission verification vulnerability in the wpa_supplicant module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	7.5	High
CVE-2024-32992	Huawei	Insufficient verification vulnerability in the baseband module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	7.5	High
CVE-2024-27942	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow any unauthenticated client to disconnect any active user from the server. An attacker could use this vulnerability to prevent any user to perform actions in the system, causing a denial of service situation.	2024-05-14	7.5	High
CVE-2024-23105	Fortinet	A Use Of Less Trusted Source [CWE-348] vulnerability in Fortinet FortiPortal version 7.0.0 through 7.0.6 and version 7.2.0 through 7.2.1 allows an unauthenticated attack to bypass IP protection through crafted HTTP or HTTPS packets.	2024-05-14	7.5	High
CVE-2024-30014	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-05-14	7.5	High
CVE-2024-30015	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-05-14	7.5	High
CVE-2024-30022	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-05-14	7.5	High
CVE-2024-30023	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-05-14	7.5	High
CVE-2024-30024	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-05-14	7.5	High
CVE-2024-30029	Microsoft	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-05-14	7.5	High
CVE-2024-30037	Microsoft	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2024-05-14	7.5	High
CVE-2024-3676	Proofpoint	The Proofpoint Encryption endpoint of Proofpoint Enterprise Protection contains an Improper Input Validation vulnerability that allows an unauthenticated remote attacker with a specially crafted HTTP request to create additional Encryption user accounts under the attacker's control. These accounts are able to send spoofed email to any users within the domains configured by the Administrator.	2024-05-14	7.5	High
CVE-2024-27943	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow a privileged user to upload generic files to the root installation directory of the system. By replacing specific files, an attacker could tamper specific files or even achieve remote code execution.	2024-05-14	7.2	High
CVE-2024-27944	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow a privileged user to upload firmware files to the root installation directory of the system. By replacing specific files, an attacker could tamper specific files or even achieve remote code execution.	2024-05-14	7.2	High
CVE-2024-27945	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The bulk import feature of the affected systems allow a privileged user to upload files to the root installation directory of the system. By replacing specific files, an attacker could tamper specific files or even achieve remote code execution.	2024-05-14	7.2	High
CVE-2024-31485	Siemens	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V5.30), SICORE Base system (All versions < V1.3.0). The web interface of affected devices is vulnerable to command injection due to missing server	2024-05-14	7.2	High

		side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.			
CVE-2023-44247	Fortinet	A double free vulnerability [CWE-415] in Fortinet FortiOS before 7.0.0 may allow a privileged attacker to execute code or commands via crafted HTTP or HTTPs requests.	2024-05-14	7.2	High
CVE-2023-45583	Fortinet	A use of externally-controlled format string in Fortinet FortiProxy versions 7.2.0 through 7.2.5, 7.0.0 through 7.0.11, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6 FortiPAM versions 1.1.0, 1.0.0 through 1.0.3 FortiOS versions 7.4.0, 7.2.0 through 7.2.5, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15 FortiSwitchManager versions 7.2.0 through 7.2.2, 7.0.0 through 7.0.2 allows attacker to execute unauthorized code or commands via specially crafted cli commands and http requests.	2024-05-14	7.2	High
CVE-2023-46714	Fortinet	A stack-based buffer overflow [CWE-121] vulnerability in Fortinet FortiOS version 7.2.1 through 7.2.6 and version 7.4.0 through 7.4.1 allows a privileged attacker over the administrative interface to execute arbitrary code or commands via crafted HTTP or HTTPs requests.	2024-05-14	7.2	High
CVE-2024-30044	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-05-14	7.2	High
CVE-2023-52719	Huawei	Privilege escalation vulnerability in the PMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-05-14	7.1	High
CVE-2023-40720	Fortinet	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiVoiceEntreprise version 7.0.0 through 7.0.1 and before 6.4.8 allows an authenticated attacker to read the SIP configuration of other users via crafted HTTP or HTTPS requests.	2024-05-14	7.1	High
CVE-2024-30033	Microsoft	Windows Search Service Elevation of Privilege Vulnerability	2024-05-14	7	High
CVE-2024-32989	Huawei	Insufficient verification vulnerability in the system sharing pop-up module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	3.3	Low
CVE-2024-32637	Siemens	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.256), Parasolid V36.0 (All versions < V36.0.208), Parasolid V36.1 (All versions < V36.1.173). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted X_T files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-05-14	3.3	Low
CVE-2024-33583	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected application contains a hidden configuration item to enable debug functionality. This could allow an authenticated local attacker to gain insight into the internal configuration of the deployment.	2024-05-14	3.3	Low
CVE-2023-47711	IBM	IBM Security Guardium 11.3, 11.4, 11.5, and 12.0 could allow an authenticated user to upload files that would cause a denial of service. IBM X-Force ID: 271526.	2024-05-14	2.7	Low
CVE-2024-27269	IBM	IBM QRadar SIEM 7.5 could allow a privileged user to configure user management that would disclose unintended sensitive information across tenants. IBM X-Force ID: 284575.	2024-05-14	6.8	Medium
CVE-2024-32999	Huawei	Cracking vulnerability in the OS security module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	6.8	Medium
CVE-2024-29997	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-29998	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-29999	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-30000	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-30001	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-30002	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-30003	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-30004	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-30005	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-30012	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium

CVE-2024-30021	Microsoft	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-05-14	6.8	Medium
CVE-2024-31488	Fortinet	An improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC version 9.4.0 through 9.4.4, 9.2.0 through 9.2.8, 9.1.0 through 9.1.10, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 7.2.0 through 7.2.3 may allow a remote authenticated attacker to perform stored and reflected cross site scripting (XSS) attack via crafted HTTP requests.	2024-05-14	6.8	Medium
CVE-2024-25967	Dell	Dell PowerScale OneFS versions 8.2.x through 9.7.0.1 contains an execution with unnecessary privileges vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2024-05-14	6.7	Medium
CVE-2023-36640	Fortinet	A use of externally-controlled format string in Fortinet FortiProxy versions 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiPAM versions 1.0.0 through 1.0.3, FortiOS versions 7.2.0, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.16 allows attacker to execute unauthorized code or commands via specially crafted commands	2024-05-14	6.7	Medium
CVE-2023-43040	IBM	IBM Spectrum Fusion HCI 2.5.2 through 2.7.2 could allow an attacker to perform unauthorized actions in RGW for Ceph due to improper bucket access. IBM X-Force ID: 266807.	2024-05-14	6.5	Medium
CVE-2024-31460	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, some of the data stored in `automation_tree_rules.php` is not thoroughly checked and is used to concatenate the SQL statement in `create_all_header_nodes()` function from `lib/api_automation.php` , finally resulting in SQL injection. Using SQL based secondary injection technology, attackers can modify the contents of the Cacti database, and based on the modified content, it may be possible to achieve further impact, such as arbitrary file reading, and even remote code execution through arbitrary file writing. Version 1.2.27 contains a patch for the issue.	2024-05-14	6.5	Medium
CVE-2023-46280	Siemens	A vulnerability has been identified in S7-PCT (All versions), Security Configuration Tool (SCT) (All versions), SIMATIC Automation Tool (All versions), SIMATIC BATCH V9.1 (All versions), SIMATIC NET PC Software (All versions), SIMATIC PCS 7 V9.1 (All versions), SIMATIC PDM V9.2 (All versions), SIMATIC Route Control V9.1 (All versions), SIMATIC STEP 7 V5 (All versions), SIMATIC WinCC OA V3.17 (All versions), SIMATIC WinCC OA V3.18 (All versions < V3.18 P025), SIMATIC WinCC OA V3.19 (All versions < V3.19 P010), SIMATIC WinCC Runtime Advanced (All versions), SIMATIC WinCC Runtime Professional V16 (All versions), SIMATIC WinCC Runtime Professional V17 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions), SIMATIC WinCC Runtime Professional V19 (All versions), SIMATIC WinCC Unified PC Runtime (All versions), SIMATIC WinCC V7.4 (All versions), SIMATIC WinCC V7.5 (All versions), SIMATIC WinCC V8.0 (All versions), SINAMICS Startdrive (All versions < V19 SP1), SINUMERIK ONE virtual (All versions < V6.23), SINUMERIK PLC Programming Tool (All versions), TIA Portal Cloud Connector (All versions < V2.0), Totally Integrated Automation Portal (TIA Portal) V15.1 (All versions), Totally Integrated Automation Portal (TIA Portal) V16 (All versions), Totally Integrated Automation Portal (TIA Portal) V17 (All versions), Totally Integrated Automation Portal (TIA Portal) V18 (All versions), Totally Integrated Automation Portal (TIA Portal) V19 (All versions < V19 Update 2). The affected applications contain an out of bounds read vulnerability. This could allow an attacker to cause a Blue Screen of Death (BSOD) crash of the underlying Windows kernel.	2024-05-14	6.5	Medium
CVE-2024-25970	Dell	Dell PowerScale OneFS versions 8.2.x through 9.7.0.1 contains an improper input validation vulnerability. A low privileged remote attacker could potentially exploit this vulnerability, leading to loss of integrity.	2024-05-14	6.5	Medium
CVE-2024-27946	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). Downloading files overwrites files with the same name in the installation directory of the affected systems. The filename for the target file can be specified, thus arbitrary files can be overwritten by an attacker with the required privileges.	2024-05-14	6.5	Medium
CVE-2024-33494	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager	2024-05-14	6.5	Medium

		(6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected components do not properly authenticate heartbeat messages. This could allow an unauthenticated remote attacker to affected the availability of secondary RTLS systems configured using a TeeRevProxy service and potentially cause loss of data generated during the time the attack is ongoing.			
CVE-2024-33495	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The affected application does not properly limit the size of specific logs. This could allow an unauthenticated remote attacker to exhaust system resources by creating a great number of log entries which could potentially lead to a denial of service condition. A successful exploitation requires the attacker to have access to specific SIMATIC RTLS Locating Manager Clients in the deployment.	2024-05-14	6.5	Medium
CVE-2024-33647	Siemens	A vulnerability has been identified in Polarion ALM (All versions < V2404.0). The Apache Lucene based query engine in the affected application lacks proper access controls. This could allow an authenticated user to query items beyond the user's allowed projects.	2024-05-14	6.5	Medium
CVE-2024-30011	Microsoft	Windows Hyper-V Denial of Service Vulnerability	2024-05-14	6.5	Medium
CVE-2024-30019	Microsoft	DHCP Server Service Denial of Service Vulnerability	2024-05-14	6.5	Medium
CVE-2024-30036	Microsoft	Windows Deployment Services Information Disclosure Vulnerability	2024-05-14	6.5	Medium
CVE-2024-30043	Microsoft	Microsoft SharePoint Server Information Disclosure Vulnerability	2024-05-14	6.5	Medium
CVE-2024-30053	Microsoft	Azure Migrate Cross-Site Scripting Vulnerability	2024-05-14	6.5	Medium
CVE-2024-30054	Microsoft	Microsoft Power BI Client JavaScript SDK Information Disclosure Vulnerability	2024-05-14	6.5	Medium
CVE-2024-4046	Huawei	Cracking vulnerability in the OS security module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	6.4	Medium
CVE-2024-4699	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DAR-8000-10 up to 20230922. This issue affects some unknown processing of the file /importhtml.php. The manipulation of the argument sql leads to deserialization. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-263747. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-05-14	6.3	Medium
CVE-2024-30208	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The "DBTest" tool of SIMATIC RTLS Locating Manager does not properly enforce access restriction. This could allow an authenticated local attacker to extract sensitive information from memory.	2024-05-14	6.3	Medium
CVE-2024-33496	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected SIMATIC RTLS Locating Manager Report Clients do not properly protect credentials that are used to authenticate to the server. This could allow an authenticated local attacker to extract the credentials and use them to escalate their access rights from the Manager to the Systemadministrator role.	2024-05-14	6.3	Medium
CVE-2024-33497	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All	2024-05-14	6.3	Medium

		versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected SIMATIC RTLS Locating Manager Track Viewer Client do not properly protect credentials that are used to authenticate to the server. This could allow an authenticated local attacker to extract the credentials and use them to escalate their access rights from the Manager to the Systemadministrator role.			
CVE-2024-30045	Microsoft	.NET and Visual Studio Remote Code Execution Vulnerability	2024-05-14	6.3	Medium
CVE-2023-52721	Huawei	The WindowManager module has a vulnerability in permission control. Impact: Successful exploitation of this vulnerability may affect confidentiality.	2024-05-14	6.2	Medium
CVE-2024-22345	IBM	IBM TXSeries for Multiplatforms 8.2 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 280192.	2024-05-14	6.2	Medium
CVE-2024-32995	Huawei	Denial of service (DoS) vulnerability in the AMS module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	6.2	Medium
CVE-2024-32996	Huawei	Privilege escalation vulnerability in the account module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	6.2	Medium
CVE-2024-25969	Dell	Dell PowerScale OneFS versions 8.2.x through 9.7.0.1 contains an allocation of resources without limits or throttling vulnerability. A local unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2024-05-14	6.2	Medium
CVE-2024-22344	IBM	IBM TXSeries for Multiplatforms 8.2 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 280191.	2024-05-14	6.1	Medium
CVE-2024-30268	Cacti	Cacti provides an operational monitoring and fault management framework. A reflected cross-site scripting vulnerability on the 1.3.x DEV branch allows attackers to obtain cookies of administrator and other users and fake their login using obtained cookies. This issue is fixed in commit a38b9046e9772612fda847b46308f9391a49891e.	2024-05-14	6.1	Medium
CVE-2024-32990	Huawei	Permission verification vulnerability in the system sharing pop-up module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	6.1	Medium
CVE-2024-25965	Dell	Dell PowerScale OneFS versions 8.2.x through 9.7.0.2 contains an external control of file name or path vulnerability. A local high privilege attacker could potentially exploit this vulnerability, leading to denial of service.	2024-05-14	6.1	Medium
CVE-2024-30059	Microsoft	Microsoft Intune for Android Mobile Application Management Tampering Vulnerability	2024-05-14	6.1	Medium
CVE-2023-38264	IBM	The IBM SDK, Java Technology Edition's Object Request Broker (ORB) 7.1.0.0 through 7.1.5.21 and 8.0.0.0 through 8.0.8.21 is vulnerable to a denial of service attack in some circumstances due to improper enforcement of the JEP 290 MaxRef and MaxDepth deserialization filters. IBM X-Force ID: 260578.	2024-05-14	5.9	Medium
CVE-2024-32998	Huawei	NULL pointer access vulnerability in the clock module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	5.9	Medium
CVE-2024-25968	Dell	Dell PowerScale OneFS versions 8.2.x through 9.7.0.2 contains a use of a broken or risky cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-05-14	5.9	Medium
CVE-2024-30046	Microsoft	Visual Studio Denial of Service Vulnerability	2024-05-14	5.9	Medium
CVE-2024-31443	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to 1.2.27, some of the data stored in `form_save()` function in `data_queries.php` is not thoroughly checked and is used to concatenate the HTML statement in `grow_right_pane_tree()` function from `lib/html.php` , finally resulting in cross-site scripting. Version 1.2.27 contains a patch for the issue.	2024-05-14	5.7	Medium
CVE-2024-32993	Huawei	Out-of-bounds access vulnerability in the memory module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	5.6	Medium
CVE-2023-50180	Fortinet	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiADC version 7.4.1 and below, version 7.2.3 and below, version 7.1.4 and below, version 7.0.5 and below, version 6.2.6 and below may allow a read-only admin to view data pertaining to other admins.	2024-05-14	5.5	Medium
CVE-2024-30008	Microsoft	Windows DWM Core Library Information Disclosure Vulnerability	2024-05-14	5.5	Medium

CVE-2024-30016	Microsoft	Windows Cryptographic Services Information Disclosure Vulnerability	2024-05-14	5.5	Medium
CVE-2024-30034	Microsoft	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	2024-05-14	5.5	Medium
CVE-2024-30039	Microsoft	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-05-14	5.5	Medium
CVE-2024-28761	IBM	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.25 and 12.0.1.0 through 12.0.12.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 285245.	2024-05-14	5.4	Medium
CVE-2024-28781	IBM	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4, and 8.0 through 8.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 285654.	2024-05-14	5.4	Medium
CVE-2024-29894	Cacti	Cacti provides an operational monitoring and fault management framework. Versions of Cacti prior to 1.2.27 contain a residual cross-site scripting vulnerability caused by an incomplete fix for CVE-2023-50250. `raise_message_javascript` from `lib/functions.php` now uses purify.js to fix CVE-2023-50250 (among others). However, it still generates the code out of unescaped PHP variables `$title` and `$header`. If those variables contain single quotes, they can be used to inject JavaScript code. An attacker exploiting this vulnerability could execute actions on behalf of other users. This ability to impersonate users could lead to unauthorized changes to settings. Version 1.2.27 fixes this issue.	2024-05-14	5.4	Medium
CVE-2024-30055	Microsoft	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-05-14	5.4	Medium
CVE-2024-30041	Microsoft	Microsoft Bing Search Spoofing Vulnerability	2024-05-14	5.4	Medium
CVE-2024-30050	Microsoft	Windows Mark of the Web Security Feature Bypass Vulnerability	2024-05-14	5.4	Medium
CVE-2024-25966	Dell	Dell PowerScale OneFS versions 8.2.x through 9.7.0.2 contains an improper handling of unexpected data type vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2024-05-14	5.3	Medium
CVE-2024-27947	Siemens	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems could allow log messages to be forwarded to a specific client under certain circumstances. An attacker could leverage this vulnerability to forward log messages to a specific compromised client.	2024-05-14	5.3	Medium
CVE-2024-31486	Siemens	A vulnerability has been identified in OPUPI0 AMQP/MQTT (All versions < V5.30). The affected devices stores MQTT client passwords without sufficient protection on the devices. An attacker with remote shell access or physical access could retrieve the credentials leading to confidentiality loss.	2024-05-14	5.3	Medium
CVE-2024-33498	Siemens	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected applications do not properly release memory that is allocated when handling specifically crafted incoming packets. This could allow an unauthenticated remote attacker to cause a denial of service condition by crashing the service when it runs out of memory. The service is restarted automatically after a short time.	2024-05-14	5.3	Medium
CVE-2024-4810	Linux	In register_device, the return value of ida_simple_get is unchecked, in witch ida_simple_get will use an invalid index value. To address this issue, index should be checked after ida_simple_get. When the index value is abnormal, a warning message should be printed, the port should be dropped, and the value should be recorded.	2024-05-14	5.3	Medium
CVE-2024-26007	Fortinet	An improper check or handling of exceptional conditions vulnerability [CWE-703] in Fortinet FortiOS version 7.4.1 allows an unauthenticated attacker to provoke a denial of service on the administrative interface via crafted HTTP requests.	2024-05-14	5.3	Medium
CVE-2023-45586	Fortinet	An insufficient verification of data authenticity vulnerability [CWE-345] in Fortinet FortiOS SSL-VPN tunnel mode version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.7 and before 7.0.12 & FortiProxy SSL-VPN tunnel mode version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.7 and before 7.0.13 allows an	2024-05-14	5	Medium

		authenticated VPN user to send (but not receive) packets spoofing the IP of another user via crafted network packets.			
CVE-2024-0862	Proofpoint	The Proofpoint Encryption endpoint of Proofpoint Enterprise Protection contains a Server-Side Request Forgery vulnerability that allows an authenticated user to relay HTTP requests from the Protection server to otherwise private network addresses.	2024-05-14	5	Medium
CVE-2023-52383	Huawei	Double-free vulnerability in the RSMC module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	4.7	Medium
CVE-2023-52384	Huawei	Double-free vulnerability in the RSMC module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	4.7	Medium
CVE-2024-31444	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, some of the data stored in `automation_tree_rules_form_save()` function in `automation_tree_rules.php` is not thoroughly checked and is used to concatenate the HTML statement in `form_confirm()` function from `lib/html.php` , finally resulting in cross-site scripting. Version 1.2.27 contains a patch for the issue.	2024-05-14	4.6	Medium
CVE-2024-31458	Cacti	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, some of the data stored in `form_save()` function in `graph_template_inputs.php` is not thoroughly checked and is used to concatenate the SQL statement in `draw_nontemplated_fields_graph_item()` function from `lib/html_form_templates.php` , finally resulting in SQL injection. Version 1.2.27 contains a patch for the issue.	2024-05-14	4.6	Medium
CVE-2024-28760	IBM	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.25 and 12.0.1.0 through 12.0.12.0 dashboard is vulnerable to a denial of service due to improper restrictions of resource allocation. IBM X-Force ID: 285244.	2024-05-14	4.3	Medium
CVE-2023-52720	Huawei	Race condition vulnerability in the soundtrigger module Impact: Successful exploitation of this vulnerability will affect availability.	2024-05-14	4.1	Medium
CVE-2024-22343	IBM	IBM TXSeries for Multiplatforms 8.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 280190.	2024-05-14	4	Medium
CVE-2024-4947	Google	Type Confusion in V8 in Google Chrome prior to 125.0.6422.60 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2024-05-15	8.8	High
CVE-2024-30284	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-30310	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-34094	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-34095	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-34096	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-34097	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-34098	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-34099	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current	2024-05-15	7.8	High

		user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2024-34100	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	7.8	High
CVE-2024-20366	Cisco	A vulnerability in the Tail-f High Availability Cluster Communications (HCC) function pack of Cisco Crosswork Network Services Orchestrator (NSO) could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability exists because a user-controlled search path is used to locate executable files. An attacker could exploit this vulnerability by configuring the application in a way that causes a malicious file to be executed. A successful exploit could allow the attacker to execute arbitrary code on an affected device as the root user. To exploit this vulnerability, the attacker would need valid credentials on an affected device.	2024-05-15	7.8	High
CVE-2024-20391	Cisco	A vulnerability in the Network Access Manager (NAM) module of Cisco Secure Client could allow an unauthenticated attacker with physical access to an affected device to elevate privileges to SYSTEM. This vulnerability is due to a lack of authentication on a specific function. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges on an affected device.	2024-05-15	6.8	Medium
CVE-2024-20258	Cisco	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager and Secure Email Gateway could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-05-15	6.1	Medium
CVE-2024-20392	Cisco	A vulnerability in the web-based management API of Cisco AsyncOS Software for Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack. This vulnerability is due to insufficient input validation of some parameters that are passed to the web-based management API of the affected system. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to perform cross-site scripting (XSS) attacks, resulting in the execution of arbitrary script code in the browser of the targeted user, or could allow the attacker to access sensitive, browser-based information.	2024-05-15	6.1	Medium
CVE-2024-30311	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	5.5	Medium
CVE-2024-30312	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	5.5	Medium
CVE-2024-34101	Adobe	Acrobat Reader versions 20.005.30574, 24.002.20736 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-15	5.5	Medium
CVE-2024-20394	Cisco	A vulnerability in Cisco AppDynamics Network Visibility Agent could allow an unauthenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to the inability to handle unexpected input. An attacker who has local device access could exploit this	2024-05-15	5.5	Medium

		vulnerability by sending an HTTP request to the targeted service. A successful exploit could allow the attacker to cause a DoS condition by stopping the Network Agent Service on the local device.			
CVE-2023-7258	Google	A denial of service exists in Gvisor Sandbox where a bug in reference counting code in mount point tracking could lead to a panic, making it possible for an attacker running as root and with permission to mount volumes to kill the sandbox. We recommend upgrading past commit 6a112c60a257dadac59962e0bc9e9b5aee70b5b6	2024-05-15	4.8	Medium
CVE-2024-20256	Cisco	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager and Secure Web Appliance could allow an authenticated, remote attacker to conduct an XSS attack against a user of the interface. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-05-15	4.8	Medium
CVE-2024-20257	Cisco	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email Gateway could allow an authenticated, remote attacker to conduct an XSS attack against a user of the interface.r This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-05-15	4.8	Medium
CVE-2024-20383	Cisco	A vulnerability in the Cisco Crosswork NSO CLI and the ConfD CLI could allow an authenticated, low-privileged, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to an incorrect privilege assignment when specific CLI commands are used. An attacker could exploit this vulnerability by executing an affected CLI command. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system.	2024-05-15	4.8	Medium
CVE-2024-20369	Cisco	A vulnerability in the web-based management interface of Cisco Crosswork Network Services Orchestrator (NSO) could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of a parameter in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website.	2024-05-15	4.7	Medium
CVE-2024-27260	IBM	IBM AIX could 7.2, 7.3, VIOS 3.1, and VIOS 4.1 allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands. IBM X-Force ID: 283985.	2024-05-16	8.4	High
CVE-2024-30314	Adobe	Dreamweaver Desktop versions 21.3 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an attacker. Exploitation of this issue does require user interaction.	2024-05-16	8.2	High
CVE-2024-20791	Adobe	Illustrator versions 28.4, 27.9.3 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-20792	Adobe	Illustrator versions 28.4, 27.9.3 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30274	Adobe	Substance3D - Painter versions 9.1.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary	2024-05-16	7.8	High

		code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2024-30275	Adobe	Adobe Aero Desktop versions 23.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30282	Adobe	Animate versions 24.0.2, 23.0.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30293	Adobe	Animate versions 24.0.2, 23.0.5 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30294	Adobe	Animate versions 24.0.2, 23.0.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30295	Adobe	Animate versions 24.0.2, 23.0.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30296	Adobe	Animate versions 24.0.2, 23.0.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30297	Adobe	Animate versions 24.0.2, 23.0.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30307	Adobe	Substance3D - Painter versions 9.1.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30288	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30289	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30290	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30291	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-30292	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	7.8	High
CVE-2024-20326	Cisco	A vulnerability in the ConfD CLI and the Cisco Crosswork Network Services Orchestrator CLI could allow an authenticated, low-privileged, local attacker to read and write arbitrary files as root on the underlying operating system. This vulnerability is due to improper authorization enforcement when specific CLI commands are used. An attacker could exploit this vulnerability by executing an affected CLI command with crafted arguments. A successful exploit could allow the attacker to	2024-05-16	7.8	High

		read or write arbitrary files on the underlying operating system with the privileges of the root user.			
CVE-2024-20389	Cisco	A vulnerability in the ConfD CLI and the Cisco Crosswork Network Services Orchestrator CLI could allow an authenticated, low-privileged, local attacker to read and write arbitrary files as root on the underlying operating system. This vulnerability is due to improper authorization enforcement when specific CLI commands are used. An attacker could exploit this vulnerability by executing an affected CLI command with crafted arguments. A successful exploit could allow the attacker to read or write arbitrary files on the underlying operating system with the privileges of the root user.	2024-05-16	7.8	High
CVE-2024-1417	WatchGuard	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in WatchGuard AuthPoint Password Manager on MacOS allows an a adversary with local access to execute code under the context of the AuthPoint Password Manager application. This issue affects AuthPoint Password Manager for MacOS versions before 1.0.6.	2024-05-16	7.8	High
CVE-2024-30060	Microsoft	Azure Monitor Agent Elevation of Privilege Vulnerability	2024-05-16	7.8	High
CVE-2024-4844	Trellix	Hardcoded credentials vulnerability in Trellix ePolicy Orchestrator (ePO) on Premise prior to 5.10 Service Pack 1 Update 2 allows an attacker with admin privileges on the ePO server to read the contents of the orion.keystore file, allowing them to access the ePO database encryption key. This was possible through using a hard coded password for the keystore. Access Control restrictions on the file mean this would not be exploitable unless the user is the system admin for the server that ePO is running on.	2024-05-16	7.5	High
CVE-2024-3286	Lenovo	A buffer overflow vulnerability was identified in some Lenovo printers that could allow an unauthenticated user to trigger a device restart by sending a specially crafted web request.	2024-05-16	7.5	High
CVE-2024-4960	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical has been found in D-Link DAR-7000-40 V31R02B1413C. Affected is an unknown function of the file interface/sysmanage/licenseauthorization.php. The manipulation of the argument file_upload leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-264528. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-05-16	6.3	Medium
CVE-2024-4961	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DAR-7000-40 V31R02B1413C. Affected by this vulnerability is an unknown functionality of the file /user/onlineuser.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-264529 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-05-16	6.3	Medium
CVE-2024-4962	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DAR-7000-40 V31R02B1413C. Affected by this issue is some unknown functionality of the file /useratte/resmanage.php. The manipulation of the argument file leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-264530 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-05-16	6.3	Medium
CVE-2024-4963	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DAR-7000-40 V31R02B1413C. This affects an unknown part of the file /url/url.php. The manipulation of the argument file_upload leads	2024-05-16	6.3	Medium

		to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-264531. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.			
CVE-2024-4964	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DAR-7000-40 V31R02B1413C and classified as critical. This vulnerability affects unknown code of the file /firewall/urlblist.php. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-264532. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-05-16	6.3	Medium
CVE-2024-4965	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000-40 V31R02B1413C and classified as critical. This issue affects some unknown processing of the file /useratte/resmanage.php. The manipulation of the argument load leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-264533 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-05-16	6.3	Medium
CVE-2024-20793	Adobe	Illustrator versions 28.4, 27.9.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2024-30281	Adobe	Substance3D - Designer versions 13.1.1 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2024-30298	Adobe	Animate versions 24.0.2, 23.0.5 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2024-30308	Adobe	Substance3D - Painter versions 9.1.2 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2024-30309	Adobe	Substance3D - Painter versions 9.1.2 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2024-30283	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2024-30286	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2024-30287	Adobe	Adobe Framemaker versions 2020.5, 2022.3 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-16	5.5	Medium
CVE-2023-47717	IBM	IBM Security Guardium 12.0 could allow a privileged user to perform unauthorized actions that could lead to a denial of service. IBM X-Force ID: 271690.	2024-05-16	4.4	Medium

CVE-2024-4843	Trellix	ePO doesn't allow a regular privileged user to delete tasks or assignments. Insecure direct object references that allow a least privileged user to manipulate the client task and client task assignments, hence escalating his/her privilege.	2024-05-16	4.3	Medium
CVE-2024-22120	Zabbix	Zabbix server can perform command execution for configured scripts. After command is executed, audit entry is added to "Audit Log". Due to "clientip" field is not sanitized, it is possible to injection SQL into "clientip" and exploit time based blind SQL injection.	2024-05-17	9.1	Critical
CVE-2024-22429	Dell	Dell BIOS contains an Improper Input Validation vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to arbitrary code execution.	2024-05-17	7.5	High
CVE-2024-31879	IBM	IBM i 7.2, 7.3, and 7.4 could allow a remote attacker to execute arbitrary code leading to a denial of service of network ports on the system, caused by the deserialization of untrusted data. IBM X-Force ID: 287539.	2024-05-18	7.5	High

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.