الهيئـــة الوطنيـــه
للأمـــن السيبـــرانى
Nat onal Cybersecurity Authority

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 5th of May to 11th 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**

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 ٥ ماي إلى ١١ ماي. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدّا: 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-2021-34947	NETGEAR	NETGEAR R7800 net-cgi Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R7800 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of the soap_block_table file. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of root. . Was ZDI-CAN-13055.	2024-05-07	8.8	High
CVE-2021-34981	Linux	Linux Kernel Bluetooth CMTP Module Double Free Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel. An attacker must first obtain the ability to execute high-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the CMTP module. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-11977.	2024-05-07	7.5	High
CVE-2021-34982	NETGEAR	NETGEAR Multiple Routers httpd Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of multiple NETGEAR routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. When parsing the strings file, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. . Was ZDI-CAN-13709.	2024-05-07	8.8	High
CVE-2021-34983	NETGEAR	NETGEAR Multiple Routers httpd Missing Authentication for Critical Function Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of multiple NETGEAR routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of authentication prior to allowing access to system configuration	2024-05-07	6.5	Medium

		information. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-13708.			
CVE-2021-34999	OpenBSD	OpenBSD Kernel Multicast Routing Uninitialized Memory Information Disclosure Vulnerability. This vulnerability allows local attackers to disclose sensitive information on affected installations of OpenBSD Kernel. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the implementation of multicast routing. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-14540.	2024-05-07	3.8	Low
CVE-2021-35000	OpenBSD	OpenBSD Kernel Multicast Routing Uninitialized Memory Information Disclosure Vulnerability. This vulnerability allows local attackers to disclose sensitive information on affected installations of OpenBSD Kernel. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the implementation of multicast routing. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-16112.	2024-05-07	3.3	Low
CVE-2022-43654	NETGEAR	NETGEAR CAX30S SSO Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR CAX30S routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the token parameter provided to the sso.php endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18227.	2024-05-07	8.8	High
CVE-2023-35748	D-Link	D-Link DAP-2622 DDP Firmware Upgrade Server IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20076.	2024-05-07	8.8	High
CVE-2023-35749	D-Link	D-Link DAP-2622 DDP Firmware Upgrade Filename Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20077.	2024-05-07	8.8	High
CVE-2023-35757	D-Link	D-Link DAP-2622 DDP Set Date-Time NTP Server Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20085.	2024-05-07	8.8	High
CVE-2023-37325	D-Link	D-Link DAP-2622 DDP Set SSID List Missing Authentication Vulnerability. This vulnerability allows network-adjacent attackers to make unauthorized changes to device configuration on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results	2024-05-07	5.4	Medium

		from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to manipulate wireless authentication settings. Was ZDI-CAN-20104.			
CVE-2023-40694	IBM	IBM Watson CP4D Data Stores 4.0.0 through 4.8.4 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 264838.	2024-05-07	6.2	Medium
CVE-2024-27273	IBM	IBM AIX's Unix domain (AIX 7.2, 7.3, VIOS 3.1, and VIOS 4.1) datagram socket implementation could potentially expose applications using Unix domain datagram sockets with SO_PEERID operation and may lead to privilege escalation. IBM X-Force ID: 284903.	2024-05-07	8.1	High
CVE-2024-21793	F5	An OData injection vulnerability exists in the BIG-IP Next Central Manager API (URI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	7.5	High
CVE-2024-22264	VMware	VMware Avi Load Balancer contains a privilege escalation vulnerability. A malicious actor with admin privileges on VMware Avi Load Balancer can create, modify, execute and delete files as a root user on the host system.	2024-05-08	7.2	High
CVE-2024-22266	VMware	VMware Avi Load Balancer contains an information disclosure vulnerability. A malicious actor with access to the system logs can view cloud connection credentials in plaintext.	2024-05-08	6.5	Medium
CVE-2024-22460	Dell	Dell PowerProtect DM5500 version 5.15.0.0 and prior contains an insecure deserialization Vulnerability. A remote attacker with high privileges could potentially exploit this vulnerability, leading to arbitrary code execution on the vulnerable application.	2024-05-08	2.2	Low
CVE-2024-24908	Dell	Dell PowerProtect DM5500 version 5.15.0.0 and prior contain an Arbitrary File Delete via Path Traversal vulnerability. A remote attacker with high privileges could potentially exploit this vulnerability to deletion of arbitrary files stored on the server filesystem.	2024-05-08	6.5	Medium
CVE-2024-25560	F5	When BIG-IP AFM is licensed and provisioned, undisclosed DNS traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	7.5	High
CVE-2024-26026	F5	An SQL injection vulnerability exists in the BIG-IP Next Central Manager API (URI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-05-08	7.5	High
CVE-2024-27202	F5	A DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	4.7	Medium
CVE-2024-28132	F5	Exposure of Sensitive Information vulnerability exists in the GSLB container, which may allow an authenticated attacker with local access to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	4.4	Medium
CVE-2024-28883	F5	An origin validation vulnerability exists in BIG-IP APM browser network access VPN client for Windows, macOS and Linux which may allow an attacker to bypass F5 endpoint inspection. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	7.4	High
CVE-2024-28889	F5	When an SSL profile with alert timeout is configured with a non-default value on a virtual server, undisclosed traffic along with conditions beyond the attacker's control can cause the Traffic	2024-05-08	5.9	Medium

		Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.			
CVE-2024-28971	Dell	Dell Update Manager Plugin, versions 1.4.0 through 1.5.0, contains a Plain-text Password Storage Vulnerability in Log file. A remote high privileged attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2024-05-08	3.5	Low
CVE-2024-31156	F5	A stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	8	High
CVE-2024-32049	F5	BIG-IP Next Central Manager (CM) may allow an unauthenticated, remote attacker to obtain the BIG-IP Next LTM/WAF instance credentials. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	7.4	High
CVE-2024-32761	F5	Under certain conditions, a potential data leak may occur in the Traffic Management Microkernels (TMMs) of BIG-IP tenants running on VELOS and rSeries platforms. However, this issue cannot be exploited by an attacker because it is not consistently reproducible and is beyond an attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-05-08	6.5	Medium
CVE-2024-33604	F5	A reflected cross-site scripting (XSS) vulnerability exist in undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-05-08	6.1	Medium
CVE-2024-33608	F5	When IPsec is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	7.5	High
CVE-2024-33612	F5	An improper certificate validation vulnerability exists in BIG-IP Next Central Manager and may allow an attacker to impersonate an Instance Provider system. A successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-05-08	6.8	Medium

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.