الهيئة الوطنية للأمن السيبراني
National 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 2nd of June to 8th of June. 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 ٢ يونيو إلى ٨ يونيو. 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-2024-29972 | Zyxel | The command injection vulnerability in the CGI program "remote_help-cgi" in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request | 2024-06-04 | 9.8 | Critical |
| CVE-2024-29973 | Zyxel | The command injection vulnerability in the “setCookie” parameter in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request | 2024-06-04 | 9.8 | Critical |
| CVE-2024-29974 | Zyxel | The remote code execution vulnerability in the CGI program “file_upload-cgi” in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an unauthenticated attacker to execute arbitrary code by uploading a crafted configuration file to a vulnerable device | 2024-06-04 | 9.8 | Critical |
| CVE-2024-5526 | Grafana | Grafana OnCall is an easy-to-use on-call management tool that will help reduce toil in on-call management through simpler workflows and interfaces that are tailored specifically for engineers.<br>Grafana OnCall, from version 1.1.37 before 1.5.2 are vulnerable to a Server Side Request Forgery (SSRF) vulnerability in the webhook functionallity.<br>This issue was fixed in version 1.5.2 | 2024-06-05 | 9.1 | Critical |
| CVE-2024-23668 | Fortinet | An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. | 2024-06-03 | 8.8 | High |
| CVE-2024-23669 | Fortinet | An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. | 2024-06-05 | 8.8 | High |
| CVE-2024-5505 | NETGEAR | NETGEAR ProSAFE Network Management System UpLoadServlet Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability.<br>The specific flaw exists within the UpLoadServlet class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-22724. | 2024-06-06 | 8.8 | High |
| CVE-2023-45192 | IBM | IBM Engineering Requirements Management DOORS Next 7.0.2 and 7.0.3 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit | 2024-06-06 | 8.2 | High |

| | | | | | |
|---|---|---|---|---|---|
| | | this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 268758. | | | |
| CVE-2024-29170 | Dell | Dell PowerScale OneFS versions 8.2.x through 9.8.0.x contain a use of hard coded credentials vulnerability. An adjacent network unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure of network traffic and denial of service. | 2024-06-04 | 8.1 | High |
| CVE-2024-28996 | SolarWinds | The SolarWinds Platform was determined to be affected by a SWQL Injection Vulnerability. Attack complexity is high for this vulnerability. | 2024-06-04 | 8.1 | High |
| CVE-2024-23667 | Fortinet | An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. | 2024-06-03 | 7.8 | High |
| CVE-2024-23670 | Fortinet | An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. | 2024-06-03 | 7.8 | High |
| CVE-2023-32475 | Dell | Dell BIOS contains a missing support for integrity check vulnerability. An attacker with physical access to the system could potentially bypass security mechanisms to run arbitrary code on the system. | 2024-06-07 | 7.6 | High |
| CVE-2024-29975 | Zyxel | The improper privilege management vulnerability in the SUID executable binary in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an authenticated local attacker with administrator privileges to execute some system commands as the “root” user on a vulnerable device | 2024-06-04 | 6.7 | Medium |
| CVE-2024-31493 | Fortinet | An improper removal of sensitive information before storage or transfer vulnerability [CWE-212] in FortiSOAR version 7.3.0, version 7.2.2 and below, version 7.0.3 and below may allow an authenticated low privileged user to read Connector passwords in plain-text via HTTP responses. | 2024-06-03 | 6.5 | Medium |
| CVE-2024-29976 | Zyxel | The improper privilege management vulnerability in the command “show_allsessions” in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an authenticated attacker to obtain a logged-in administrator’s session information containing cookies on an affected device | 2024-06-04 | 6.5 | Medium |
| CVE-2024-5463 | Synology | A vulnerability regarding buffer copy without checking the size of input ('Classic Buffer Overflow') has been found in the login component. This allows remote attackers to conduct denial-of-service attacks via unspecified vectors. This attack only affects the login service which will automatically restart. The following models with Synology Camera Firmware versions before 1.1.1-0383 may be affected: BC500 and TC500. | 2024-06-04 | 6.5 | Medium |
| CVE-2024-23664 | Fortinet | A URL redirection to untrusted site ('open redirect') in Fortinet FortiAuthenticator version 6.6.0, version 6.5.3 and below, version 6.4.9 and below may allow an attacker to to redirect users to an arbitrary website via a crafted URL. | 2024-06-03 | 6.1 | Medium |
| CVE-2024-23665 | Fortinet | Multiple improper authorization vulnerabilities [CWE-285] in FortiWeb version 7.4.2 and below, version 7.2.7 and below, version 7.0.10 and below, version 6.4.3 and below, version 6.3.23 and below may allow an authenticated attacker to perform unauthorized ADOM operations via crafted requests. | 2024-06-03 | 5.9 | Medium |
| CVE-2024-23107 | Fortinet | An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiWeb version 7.4.0, version 7.2.4 and below, version 7.0.8 and below, 6.3 all versions may allow an authenticated attacker to read password hashes of other administrators via CLI commands. | 2024-06-03 | 5.5 | Medium |
| CVE-2024-20404 | Cisco | A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system.<br>This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device. | 2024-06-05 | 5.3 | Medium |
| CVE-2024-31878 | IBM | IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538. | 2024-06-07 | 5.3 | Medium |
| CVE-2024-22326 | IBM | IBM System Storage DS8900F 89.22.19.0, 89.30.68.0, 89.32.40.0, 89.33.48.0, 89.40.83.0, and 89.40.93.0 could allow a remote user to create an LDAP connection with a valid username and empty | 2024-06-06 | 5 | Medium |

| | | | | | |
|---|---|---|---|---|---|
| | | password to establish an anonymous connection. IBM X-Force ID: 279518. | | | |
| CVE-2024-20405 | Cisco | A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability.<br>This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user 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 information on the affected device. | 2024-06-05 | 4.8 | Medium |
| CVE-2023-48789 | Fortinet | A client-side enforcement of server-side security in Fortinet FortiPortal version 6.0.0 through 6.0.14 allows attacker to improper access control via crafted HTTP requests. | 2024-06-03 | 4.3 | 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.**