Últimas 10 Vulnerabilidades

Id	Descripción	Fecha Publicación	Fecha Modificación	Puntuación CVSS
CVE-2023-5675	A flaw was found in Quarkus. When a Quarkus RestEasy Classic or Reactive JAX-RS endpoint has its methods declared in the abstract Java class or customized by Quarkus extensions using the annotation processor, the authorization of these methods will not be enforced if it is enabled by either 'quarkus.security.jaxrs.deny-unannotated-endpoints' or 'quarkus.security.jaxrs.default-roles-allowed' properties.	25/04/2024 - 16:15:00	25/04/2024 - 17:25:00	None
CVE-2023-6484	A log injection flaw was found in Keycloak. A text string may be injected through the authentication form when using the WebAuthn authentication mode. This issue may have a minor impact to the logs integrity.	25/04/2024 - 16:15:00	25/04/2024 - 17:25:00	None
CVE-2024-4006	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.7 before 16.9.6, all versions starting from 16.10 before 16.10.4, all versions starting from 16.11 before 16.11.1 where personal access scopes were not honored by GraphQL subscriptions	25/04/2024 - 14:15:00	25/04/2024 - 17:25:00	None
CVE-2024-4024	An issue has been discovered in GitLab CE/EE affecting all versions starting from 7.8 before 16.9.6, all versions starting from 16.10 before 16.10.4, all versions starting from 16.11 before 16.11.1. Under certain conditions, an attacker with their Bitbucket account credentials may be able to take over a GitLab account linked to another user's Bitbucket account, if Bitbucket is used as an OAuth 2.0 provider on GitLab.	25/04/2024 - 14:15:00	25/04/2024 - 17:25:00	None
CVE-2024-4171	A vulnerability classified as critical has been found in Tenda W30E 1.0/1.0.1.25. Affected is the function fromWizardHandle of the file /goform/WizardHandle. The manipulation of the argument PPW leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-261990 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	25/04/2024 - 14:15:00	25/04/2024 - 17:25:00	None
CVE-2024-4172	A vulnerability classified as problematic was found in idcCMS 1.35. Affected by this vulnerability is an unknown functionality of the file /admin/admin_cl.php?mudi=revPwd. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-261991.	25/04/2024 - 14:15:00	25/04/2024 - 17:25:00	None
CVE-2024-22373	An out-of-bounds write vulnerability exists in the JPEG2000Codec::DecodeByStreamsCommon functionality of Mathieu Malaterre Grassroot DICOM 3.0.23. A specially crafted DICOM file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	25/04/2024 - 15:16:00	25/04/2024 - 17:25:00	None
CVE-2024-22391	A heap-based buffer overflow vulnerability exists in the LookupTable::SetLUT functionality of Mathieu Malaterre Grassroot DICOM 3.0.23. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	25/04/2024 - 15:16:00	25/04/2024 - 17:25:00	None
CVE-2024-25569	An out-of-bounds read vulnerability exists in the RAWCodec::DecodeBytes functionality of Mathieu Malaterre Grassroot DICOM 3.0.23. A specially crafted DICOM file can lead to an out-of-bounds read. An attacker can provide a malicious file to trigger this vulnerability.	25/04/2024 - 15:16:00	25/04/2024 - 17:25:00	None
CVE-2024-33592	Server-Side Request Forgery (SSRF) vulnerability in SoftLab Radio Player.This issue affects Radio Player: from n/a through 2.0.73.	25/04/2024 - 15:16:00	25/04/2024 - 17:25:00	None