Últimas 10 Vulnerabilidades

Id	Descripción	Fecha Publicación	Fecha Modificación	Puntuación CVSS
CVE-2024-4165	A vulnerability, which was classified as critical, was found in Tenda G3 15.11.0.17(9502). Affected is the function modifyDhcpRule of the file /goform/modifyDhcpRule. The manipulation of the argument bindDhcpIndex 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. The identifier of this vulnerability is VDB-261984. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	25/04/2024 - 12:15:00	25/04/2024 - 13:18:00	None
CVE-2024-4166	A vulnerability has been found in Tenda 4G300 1.01.42 and classified as critical. Affected by this vulnerability is the function sub_41E858. The manipulation of the argument GO/page leads to stack-based buffer overflow. The attack can be launched remotely. The identifier VDB-261985 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	25/04/2024 - 12:15:00	25/04/2024 - 13:18:00	None
CVE-2024-4167	A vulnerability was found in Tenda 4G300 1.01.42 and classified as critical. Affected by this issue is the function sub_422AA4. The manipulation of the argument year/month/day/hour/minute/second leads to stack-based buffer overflow. The attack may be launched remotely. VDB-261986 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 - 12:15:00	25/04/2024 - 13:18:00	None
CVE-2024-4168	A vulnerability was found in Tenda 4G300 1.01.42. It has been classified as critical. This affects the function sub_4260F0. The manipulation of the argument upfilen leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-261987. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	25/04/2024 - 12:15:00	25/04/2024 - 13:18:00	None
CVE-2024-4174	Cross-Site Scripting (XSS) vulnerability in Hyperion Web Server affecting version 2.0.15. This vulnerability could allow an attacker to execute malicious Javascript code on the client by injecting that code into the URL.	25/04/2024 - 12:15:00	25/04/2024 - 13:18:00	None
CVE-2024-4175	Unicode transformation vulnerability in Hyperion affecting version 2.0.15. This vulnerability could allow an attacker to send a malicious payload with Unicode characters that will be replaced by ASCII characters.	25/04/2024 - 12:15:00	25/04/2024 - 13:18:00	None
CVE-2023-3597	A flaw was found in Keycloak, where it does not correctly validate its client step-up authentication in org.keycloak.authentication. This flaw allows a remote user authenticated with a password to register a false second authentication factor along with an existing one and bypass authentication.	25/04/2024 - 13:15:00	25/04/2024 - 13:18:00	None
CVE-2024-25026	IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.4 are vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 281516.	25/04/2024 - 13:15:00	25/04/2024 - 13:18:00	None
CVE-2024-33247	Sourcecodester Employee Task Management System v1.0 is vulnerable to SQL Injection via admin-manage-user.php.	25/04/2024 - 13:15:00	25/04/2024 - 13:18:00	None
CVE-2024-4169	A vulnerability was found in Tenda 4G300 1.01.42. It has been declared as critical. This vulnerability affects the function sub_42775C/sub_4279CC. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be initiated remotely. The identifier of this vulnerability is VDB-261988. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	25/04/2024 - 13:15:00	25/04/2024 - 13:18:00	None