CVEs más relevantes de la semana

Del 20/09/2025 al 27/09/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-10779

Descripción: A vulnerability was found in D-Link DCS-935L up to 1.13.01. The impacted element is the function sub_402280 of the file /HNAP1/. The manipulation of the argument HNAP_AUTH/SOAPAction results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.

CVSS: 8.8 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10781

Descripción: A vulnerability was identified in Campcodes Online Learning Management System 1.0. This impacts an unknown function of the file /admin/edit_class.php. Such manipulation of the argument class_name leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10782

Descripción: A security flaw has been discovered in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/class.php. Performing manipulation of the argument class_name results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10783

Descripción: A weakness has been identified in Campcodes Online Learning Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add_subject.php. Executing manipulation of the argument subject_code can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10784

Descripción: A security vulnerability has been detected in Campcodes Online Learning Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_subject.php. The manipulation of the argument subject_code leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10785

Descripción: A vulnerability was detected in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown part of the file /manage_user.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10786

Descripción: A flaw has been found in Campcodes Grocery Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=delete_user. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10788

Descripción: A vulnerability was determined in SourceCodester Online Hotel Reservation System 1.0. The affected element is an unknown function of the file deleteroominventory.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10789

Descripción: A vulnerability was identified in SourceCodester Online Hotel Reservation System 1.0. The impacted element is an unknown function of the file deleteslide.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10791

Descripción: A weakness has been identified in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/index.php. This manipulation of the argument aduser causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10793

Descripción: A vulnerability was detected in code-projects E-Commerce Website 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/admin_account_delete.php. Performing manipulation of the argument user_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10795

Descripción: A vulnerability has been found in code-projects Online Bidding System 1.0. This affects an unknown part of the file /administrator/bidupdate.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10796

Descripción: A vulnerability was found in code-projects Hostel Management System 1.0. This vulnerability affects unknown code of the file /justines/admin/login.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10797

Descripción: A vulnerability was determined in code-projects Hostel Management System 1.0. This issue affects some unknown processing of the file /justines/index.php. This manipulation of the argument log_email causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10798

Descripción: A vulnerability was identified in code-projects Hostel Management System 1.0. Impacted is an unknown function of the file /justines/admin/mod_roomtype/index.php?view=view. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10799

Descripción: A security flaw has been discovered in code-projects Hostel Management System 1.0. The affected element is an unknown function of the file /justines/admin/mod_reservation/index.php?view=view. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10800

Descripción: A weakness has been identified in itsourcecode Online Discussion Forum 1.0. The impacted element is an unknown function of the file /index.php. Executing manipulation of the argument email/password can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10801

Descripción: A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown function of the file /admin/edit_tax.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10802

Descripción: A flaw has been found in code-projects Online Bidding System 1.0. Affected is an unknown function of the file /administrator/remove.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10808

Descripción: A weakness has been identified in Campcodes Farm Management System 1.0. Impacted is an unknown function of the file /uploadProduct.php. This manipulation of the argument Type causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10809

Descripción: A security vulnerability has been detected in Campcodes Online Learning Management System 1.0. The affected element is an unknown function of the file /admin/department.php. Such manipulation of the argument d leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10810

Descripción: A vulnerability was detected in Campcodes Online Learning Management System 1.0. The impacted element is an unknown function of the file /admin/edit_user.php. Performing manipulation of the argument firstname results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10811

Descripción: A flaw has been found in code-projects Hostel Management System 1.0. This affects an unknown function of the file /justines/admin/mod_comments/index.php?view=view. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10812

Descripción: A vulnerability has been found in code-projects Hostel Management System 1.0. This impacts an unknown function of the file /justines/admin/mod_amenities/index.php?view=view. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10813

Descripción: A vulnerability was found in code-projects Hostel Management System 1.0. Affected is an unknown function of the file /justines/admin/mod_reports/index.php. The manipulation of the argument Home results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10817

Descripción: A weakness has been identified in Campcodes Online Learning Management System 1.0. This vulnerability affects unknown code of the file /admin/admin_user.php. Executing manipulation of the argument firstname can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-22

CVE-2025-10829

Descripción: A vulnerability was detected in Campcodes Computer Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/sup_edit1.php. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10830

Descripción: A flaw has been found in Campcodes Computer Sales and Inventory System 1.0. This issue affects some unknown processing of the file /pages/inv_edit1.php. Executing manipulation of the argument idd can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10831

Descripción: A vulnerability has been found in Campcodes Computer Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/pro_edit1.php. The manipulation of the argument prodcode leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10832

Descripción: A vulnerability was found in SourceCodester Pet Grooming Management Software 1.0. The affected element is an unknown function of the file /admin/fetch_product_details.php. The manipulation of the argument barcode results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10833

Descripción: A vulnerability was determined in 1000projects Bookstore Management System 1.0. The impacted element is an unknown function of the file /login.php. This manipulation of the argument unm causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10834

Descripción: A vulnerability was identified in itsourcecode Open Source Job Portal 1.0. This affects an unknown function of the file /jobportal/admin/login.php. Such manipulation of the argument user_email leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10836

Descripción: A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. Affected is an unknown function of the file /admin/print1.php. Executing manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-26399

Descripción: SolarWinds Web Help Desk was found to be susceptible to an unauthenticated AjaxProxy deserialization remote code execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability is a patch bypass of CVE-2024-28988, which in turn is a patch bypass of CVE-2024-28986.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-502

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-9321

Descripción: The WPCasa plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 1.4.1. This is due to insufficient input validation and restriction on the 'api_requests' function. This makes it possible for unauthenticated attackers to call arbitrary functions and execute code.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10841

Descripción: A security vulnerability has been detected in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/weweee.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10842

Descripción: A vulnerability was detected in code-projects Online Bidding System 1.0. Affected is an unknown function of the file /administrator/wew.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely.
The exploit is now public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10843

Descripción: A flaw has been found in Reservation Online Hotel Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /reservation/paypalpayout.php. Executing manipulation of the argument confirm can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10851

Descripción: A security flaw has been discovered in Campcodes Gym Management System 1.0. Impacted is an unknown function of the file /ajax.php?action=login. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-9588

Descripción: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Iron Mountain Archiving Services Inc. EnVision allows Command Injection.This issue affects enVision: before 250563.

CVSS: 10.0 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Tipo: CWE-78

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10147

Descripción: The Podlove Podcast Publisher plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'move_as_original_file' function in all versions up to, and including, 4.2.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10857

Descripción: A security flaw has been discovered in Campcodes Point of Sale System POS 1.0. Affected by this issue is some unknown functionality of the file /login.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10412

Descripción: The Product Options and Price Calculation Formulas for WooCommerce – Uni CPO (Premium) plugin for WordPress is vulnerable to arbitrary file uploads due to misconfigured file type validation in the 'uni_cpo_upload_file' function in all versions up to, and including, 4.9.54. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-9846

Descripción: Unrestricted Upload of File with Dangerous Type vulnerability in TalentSys Consulting Information Technology Industry Inc. Inka.Net allows Command Injection.This issue affects Inka.Net: before 6.7.1.

CVSS: 10.0 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-41715

Descripción: The database for the web application is exposed without authentication, allowing an unauthenticated remote attacker to gain unauthorized access and potentially compromise it.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-306

Tecnología: No especificado

Publicado el: 2025-09-24

CVE-2025-9054

Descripción: The MultiLoca - WooCommerce Multi Locations Inventory Management plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'wcmlim_settings_ajax_handler' function in all versions up to, and including, 4.2.8. This makes it possible for unauthenticated attackers to update arbitrary options on the WordPres...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-09-24

CVE-2025-21483

Descripción: Memory corruption when the UE receives an RTP packet from the network, during the reassembly of NALUs.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-09-24

CVE-2025-27034

Descripción: Memory corruption while selecting the PLMN from SOR failed list.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-129

Tecnología: No especificado

Publicado el: 2025-09-24

CVE-2025-20363

Descripción: A vulnerability in the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, remote attacker (Cisco ASA and FTD Software) or authenticated, remote attacker (Cisco IOS, IOS XE, and IOS XR Software) with low user priv...

CVSS: 9.0 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Tipo: CWE-122

Tecnología: No especificado

Publicado el: 2025-09-25

Resumen del Reporte

CVEs analizados: 49

Promedio CVSS: 7.88

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat