CVEs más relevantes de la semana

Del 12/07/2025 al 19/07/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-7471

Descripción: A vulnerability was found in code-projects Modern Bag 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/login-back.php. The manipulation of the argument user-name leads to sql injection. The attack can be launched 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: 2025-07-12

CVE-2025-7474

Descripción: A vulnerability was found in code-projects Job Diary 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /search.php. The manipulation of the argument Search leads to sql injection. The attack may be launched 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: 2025-07-12

CVE-2025-7475

Descripción: A vulnerability classified as critical has been found in code-projects Simple Car Rental System 1.0. This affects an unknown part of the file /pay.php. The manipulation of the argument mpesa 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: 2025-07-12

CVE-2025-7476

Descripción: A vulnerability classified as critical was found in code-projects Simple Car Rental System 1.0. This vulnerability affects unknown code of the file /admin/approve.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: 2025-07-12

CVE-2025-7478

Descripción: A vulnerability, which was classified as critical, was found in code-projects Modern Bag 1.0. Affected is an unknown function of the file /admin/category-list.php. The manipulation of the argument idCate leads to sql injection. It is possible to launch 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: 2025-07-12

CVE-2025-7480

Descripción: A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13 and classified as critical. Affected by this issue is some unknown functionality of the file /users/signup.php. The manipulation of the argument email leads to sql injection. The attack may be launched 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: 2025-07-12

CVE-2025-7483

Descripción: A vulnerability was found in PHPGurukul Vehicle Parking Management System 1.13. It has been rated as critical. This issue affects some unknown processing of the file /users/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack may 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: 2025-07-12

CVE-2025-7508

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Modern Bag 1.0. Affected by this issue is some unknown functionality of the file /admin/product-update.php. The manipulation of the argument idProduct leads to sql injection. The attack may be launched 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: 2025-07-13

CVE-2025-7509

Descripción: A vulnerability, which was classified as critical, was found in code-projects Modern Bag 1.0. This affects an unknown part of the file /admin/slide.php. The manipulation of the argument idSlide 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: 2025-07-13

CVE-2025-7510

Descripción: A vulnerability has been found in code-projects Modern Bag 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/productadd_back.php. The manipulation of the argument namepro 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: 2025-07-13

CVE-2025-7512

Descripción: A vulnerability was found in code-projects Modern Bag 1.0. It has been classified as critical. Affected is an unknown function of the file /contact-back.php. The manipulation of the argument contact-name leads to sql injection. It is possible to launch 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: 2025-07-13

CVE-2025-7513

Descripción: A vulnerability was found in code-projects Modern Bag 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/slideupdate.php. The manipulation of the argument idSlide leads to sql injection. The attack can be launched 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: 2025-07-13

CVE-2025-7514

Descripción: A vulnerability was found in code-projects Modern Bag 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/contact-list.php. The manipulation of the argument idStatus leads to sql injection. The attack may be launched 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: 2025-07-13

CVE-2025-7515

Descripción: A vulnerability classified as critical has been found in code-projects Online Appointment Booking System 1.0. This affects an unknown part of the file /ulocateus.php. The manipulation of the argument doctorname 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: 2025-07-13

CVE-2025-7516

Descripción: A vulnerability classified as critical was found in code-projects Online Appointment Booking System 1.0. This vulnerability affects unknown code of the file /cancelbookingpatient.php. The manipulation of the argument appointment 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: 2025-07-13

CVE-2025-7517

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /getDay.php. The manipulation of the argument cidval leads to sql injection. The attack may 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: 2025-07-13

CVE-2025-7521

Descripción: A vulnerability, which was classified as critical, was found in PHPGurukul Vehicle Parking Management System 1.13. Affected is an unknown function of the file /admin/index.php. The manipulation of the argument Username leads to sql injection. It is possible to launch 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: 2025-07-13

CVE-2025-7533

Descripción: A vulnerability was found in code-projects Job Diary 1.0 and classified as critical. This issue affects some unknown processing of the file /view-details.php. The manipulation of the argument job_id leads to sql injection. The attack may 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: 2025-07-13

CVE-2025-7534

Descripción: A vulnerability was found in PHPGurukul Student Result Management System 2.0. It has been classified as critical. Affected is an unknown function of the file /notice-details.php of the component GET Parameter Handler. The manipulation of the argument nid leads to sql injection. It is possible to launch 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: 2025-07-13

CVE-2025-7535

Descripción: A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /pages/reprint_cash.php. The manipulation of the argument sid leads to sql injection. The attack can be launched 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: 2025-07-13

CVE-2025-7536

Descripción: A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /pages/receipt_credit.php. The manipulation of the argument sid leads to sql injection. The attack may be launched 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: 2025-07-13

CVE-2025-7537

Descripción: A vulnerability classified as critical has been found in Campcodes Sales and Inventory System 1.0. This affects an unknown part of the file /pages/product_update.php. 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: 2025-07-13

CVE-2025-7538

Descripción: A vulnerability classified as critical was found in Campcodes Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/product_update.php. The manipulation of the argument image leads to unrestricted upload. 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-284

Tecnología: No especificado

Publicado el: 2025-07-13

CVE-2025-7539

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /getdoctordaybooking.php. The manipulation of the argument cid leads to sql injection. The attack may 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: 2025-07-13

CVE-2025-7540

Descripción: A vulnerability, which was classified as critical, was found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /getclinic.php. The manipulation of the argument townid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.

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: 2025-07-13

CVE-2025-7541

Descripción: A vulnerability has been found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /get_town.php. The manipulation of the argument countryid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affec...

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: 2025-07-13

CVE-2025-7542

Descripción: A vulnerability was found in PHPGurukul User Registration & Login and User Management System 3.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/user-profile.php. The manipulation of the argument uid leads to sql injection. The attack may be launched 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: 2025-07-13

CVE-2025-7547

Descripción: A vulnerability, which was classified as critical, was found in Campcodes Online Movie Theater Seat Reservation System 1.0. This affects the function save_movie of the file /admin/admin_class.php. The manipulation of the argument cover leads to unrestricted upload. 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-284

Tecnología: No especificado

Publicado el: 2025-07-13

CVE-2025-7587

Descripción: A vulnerability was found in code-projects Online Appointment Booking System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /cover.php. The manipulation of the argument uname/psw leads to sql injection. The attack may be launched 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: 2025-07-14

CVE-2025-7593

Descripción: A vulnerability was found in code-projects Job Diary 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view-all.php. The manipulation of the argument ID leads to sql injection. The attack may be launched 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: 2025-07-14

CVE-2025-7594

Descripción: A vulnerability was found in code-projects Job Diary 1.0. It has been classified as critical. This affects an unknown part of the file /view-emp.php. 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: 2025-07-14

CVE-2025-7595

Descripción: A vulnerability was found in code-projects Job Diary 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /view-cad.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: 2025-07-14

CVE-2025-7604

Descripción: A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /user-login.php. The manipulation of the argument Username leads to sql injection. The attack can be launched 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: 2025-07-14

CVE-2025-7605

Descripción: A vulnerability was found in code-projects AVL Rooms 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /profile.php. The manipulation of the argument first_name leads to sql injection. The attack may be launched 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: 2025-07-14

CVE-2025-7606

Descripción: A vulnerability classified as critical has been found in code-projects AVL Rooms 1.0. This affects an unknown part of the file /city.php. The manipulation of the argument city 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: 2025-07-14

CVE-2025-7607

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Simple Shopping Cart 1.0. This issue affects some unknown processing of the file /Customers/save_order.php. The manipulation of the argument order_price leads to sql injection. The attack may 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: 2025-07-14

CVE-2025-7608

Descripción: A vulnerability, which was classified as critical, was found in code-projects Simple Shopping Cart 1.0. Affected is an unknown function of the file /userlogin.php. The manipulation of the argument user_email leads to sql injection. It is possible to launch 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: 2025-07-14

CVE-2025-7609

Descripción: A vulnerability has been found in code-projects Simple Shopping Cart 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /register.php. The manipulation of the argument ruser_email leads to sql injection. The attack can be launched 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: 2025-07-14

CVE-2025-7610

Descripción: A vulnerability was found in code-projects Electricity Billing System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user/change_password.php. The manipulation of the argument new_password leads to sql injection. The attack may be launched 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: 2025-07-14

CVE-2025-7611

Descripción: A vulnerability was found in code-projects Wedding Reservation 1.0. It has been classified as critical. This affects an unknown part of the file /global.php. The manipulation of the argument lu 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: 2025-07-14

CVE-2025-7612

Descripción: A vulnerability was found in code-projects Mobile Shop 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument email 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: 2025-07-14

CVE-2025-5393

Descripción: The Alone – Charity Multipurpose Non-profit WordPress Theme theme for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the alone_import_pack_restore_data() function in all versions up to, and including, 7.8.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution ...

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-73

Tecnología: No especificado

Publicado el: 2025-07-15

CVE-2025-5394

Descripción: The Alone – Charity Multipurpose Non-profit WordPress Theme theme for WordPress is vulnerable to arbitrary file uploads due to a missing capability check on the alone_import_pack_install_plugin() function in all versions up to, and including, 7.8.3. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve...

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: 2025-07-15

CVE-2025-7340

Descripción: The HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder. plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the temp_file_upload function in all versions up to, and including, 2.2.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote co...

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: 2025-07-15

CVE-2025-7341

Descripción: The HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder. plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the temp_file_delete() function in all versions up to, and including, 2.2.1. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote...

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-269

Tecnología: No especificado

Publicado el: 2025-07-15

CVE-2025-7360

Descripción: The HT Contact Form Widget For Elementor Page Builder & Gutenberg Blocks & Form Builder. plugin for WordPress is vulnerable to arbitrary file moving due to insufficient file path validation in the handle_files_upload() function in all versions up to, and including, 2.2.1. This makes it possible for unauthenticated attackers to move arbitrary files on the server, which can easily lead to remote ...

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-07-15

CVE-2025-7673

Descripción: A buffer overflow vulnerability in the URL parser of the zhttpd web server in Zyxel VMG8825-T50K firmware versions prior to V5.50(ABOM.5)C0 could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and potentially execute arbitrary code by sending a specially crafted HTTP request.

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-120

Tecnología: No especificado

Publicado el: 2025-07-16

CVE-2024-9342

Descripción: In Eclipse GlassFish version 7.0.16 or earlier it is possible to perform Login Brute Force attacks as there is no limitation in the number of failed login attempts.

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-307

Tecnología: No especificado

Publicado el: 2025-07-16

CVE-2024-9408

Descripción: In Eclipse GlassFish since version 6.2.5 it is possible to perform a Server Side Request Forgery attack in specific endpoints.

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-918

Tecnología: No especificado

Publicado el: 2025-07-16

CVE-2025-20337

Descripción: A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit this vulnerability. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sub...

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-74

Tecnología: No especificado

Publicado el: 2025-07-16

CVE-2025-5396

Descripción: The Bears Backup plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.0.0. This is due to the bbackup_ajax_handle() function not having a capability check, nor validating user supplied input passed directly to call_user_func(). This makes it possible for unauthenticated attackers to execute code on the server which can be leverage to inject backdoo...

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: 2025-07-17

CVE-2025-7712

Descripción: The Madara - Core plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the wp_manga_delete_zip() function in all versions up to, and including, 2.2.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-07-17

CVE-2025-52046

Descripción: Totolink A3300R V17.0.0cu.596_B20250515 was found to contain a command injection vulnerability in the sub_4197C0 function via the mac and desc parameters. This vulnerability allows unauthenticated attackers to execute arbitrary commands via a crafted request.

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-77

Tecnología: No especificado

Publicado el: 2025-07-17

CVE-2025-7749

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /admin/getmanagerregion.php. The manipulation of the argument city leads to sql injection. The attack may 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: 2025-07-17

CVE-2025-7750

Descripción: A vulnerability, which was classified as critical, was found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /admin/adddoctorclinic.php. The manipulation of the argument clinic leads to sql injection. It is possible to launch 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: 2025-07-17

CVE-2025-7751

Descripción: A vulnerability has been found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/addclinic.php. The manipulation of the argument cid leads to sql injection. The attack can be launched 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: 2025-07-17

CVE-2025-7752

Descripción: A vulnerability was found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/deletedoctor.php. The manipulation of the argument did leads to sql injection. The attack may be launched 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: 2025-07-17

CVE-2025-7753

Descripción: A vulnerability was found in code-projects Online Appointment Booking System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/adddoctor.php. The manipulation of the argument Username 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: 2025-07-17

CVE-2025-6222

Descripción: The WooCommerce Refund And Exchange with RMA - Warranty Management, Refund Policy, Manage User Wallet theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'ced_rnx_order_exchange_attach_files' function in all versions up to, and including, 3.2.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site'...

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: 2025-07-18

CVE-2025-7643

Descripción: The Attachment Manager plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the handle_actions() function in all versions up to, and including, 2.1.2. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-07-18

CVE-2025-7444

Descripción: The LoginPress Pro plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 5.0.1. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not ...

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-288

Tecnología: No especificado

Publicado el: 2025-07-18

CVE-2025-47158

Descripción: Authentication bypass by assumed-immutable data in Azure DevOps allows an unauthorized attacker to elevate privileges over a network.

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-302

Tecnología: No especificado

Publicado el: 2025-07-18

CVE-2025-49746

Descripción: Improper authorization in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-285

Tecnología: No especificado

Publicado el: 2025-07-18

CVE-2025-49747

Descripción: Missing authorization in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-07-18

CVE-2025-7696

Descripción: The Integration for Pipedrive and Contact Form 7, WPForms, Elementor, Ninja Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.2.3 via deserialization of untrusted input within the verify_field_val() function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in the Contact Fo...

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: 2025-07-19

CVE-2025-7697

Descripción: The Integration for Google Sheets and Contact Form 7, WPForms, Elementor, Ninja Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.1.1 via deserialization of untrusted input within the verify_field_val() function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in the Contac...

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: 2025-07-19

CVE-2012-10019

Descripción: The Front End Editor plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation via the upload.php file in versions before 2.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites 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: 2025-07-19

CVE-2015-10135

Descripción: The WPshop 2 – E-Commerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajaxUpload function in versions before 1.3.9.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites 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: 2025-07-19

CVE-2016-15043

Descripción: The WP Mobile Detector plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in resize.php file in versions up to, and including, 3.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites 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: 2025-07-19

Resumen del Reporte

CVEs analizados: 69

Promedio CVSS: 8.08

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat