# CVEs más relevantes de la semana

Del 15/07/2025 al 22/07/2025

Porque el primer paso para defender es conocer las amenazas.

# 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

# CVE-2015-10138

Descripción: The Work The Flow File Upload plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the jQuery-File-Upload-9.5.0 server and test files in versions up to, and including, 2.5.2. 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-2025-7343

Descripción: The SFT developed by Digiwin has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

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-89

Tecnología: No especificado

Publicado el: 2025-07-21

# CVE-2025-7921

Descripción: Certain modem models developed by Askey has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated remote attackers to control the program's execution flow and potentially execute arbitrary 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-121

Tecnología: No especificado

Publicado el: 2025-07-21

# CVE-2012-10020

Descripción: The FoxyPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the uploadify.php file in versions up to, and including, 0.4.2.1. 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: 2025-07-22

# CVE-2015-10137

Descripción: The Website Contact Form With File Upload plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_file()' function in versions up to, and including, 1.3.4. 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: 2025-07-22

# CVE-2025-6187

Descripción: The bSecure plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within its order_info REST endpoint in versions 1.3.7 through 1.7.9. The plugin registers the /webhook/v2/order_info/ route with a permission_callback that always returns true, effectively bypassing all authentication. This makes it possible for unauthenticated attackers who know any user's email...

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: 2025-07-22

# CVE-2025-4285

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rolantis Information Technologies Agentis allows SQL Injection.This issue affects Agentis: before 4.32.

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-89

Tecnología: No especificado

Publicado el: 2025-07-22

# Resumen del Reporte

CVEs analizados: 30

Promedio CVSS: 9.33

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat