CVEs más relevantes de la semana

Del 08/07/2025 al 15/07/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-47981

Descripción: Heap-based buffer overflow in Windows SPNEGO Extended Negotiation allows an unauthorized attacker to execute code over a network.

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-122

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-7191

Descripción: A vulnerability has been found in code-projects Student Enrollment System 1.0 and classified as critical. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument Username 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: 2025-07-08

CVE-2025-7193

Descripción: A vulnerability was found in itsourcecode Agri-Trading Online Shopping System up to 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/suppliercontroller.php. The manipulation of the argument supplier 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: 2025-07-08

CVE-2025-49535

Descripción: ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in a Security feature bypass. An attacker could exploit this vulnerability to access sensitive information or denial of service by bypassing security measures. Exploitation of this issue does not require user interaction and sc...

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-611

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-7196

Descripción: A vulnerability was found in code-projects Jonnys Liquor 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /browse.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: 2025-07-08

CVE-2025-27203

Descripción: Adobe Connect versions 24.0 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could lead to arbitrary code execution by an attacker. Exploitation of this issue does require user interaction and scope is changed.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-502

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-49533

Descripción: Adobe Experience Manager (MS) versions 6.5.23.0 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could lead to arbitrary code execution by an attacker. Exploitation of this issue does not require user interaction. Scope is unchanged.

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: 2025-07-08

CVE-2025-7197

Descripción: A vulnerability classified as critical has been found in code-projects Jonnys Liquor 1.0. This affects an unknown part of the file /admin/delete-row.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: 2025-07-08

CVE-2025-7198

Descripción: A vulnerability classified as critical was found in code-projects Jonnys Liquor 1.0. This vulnerability affects unknown code of the file /admin/admin-area.php. The manipulation of the argument drink 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: 2025-07-08

CVE-2025-7199

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Library System 1.0. This issue affects some unknown processing of the file /notapprove.php. The manipulation of the argument 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: 2025-07-08

CVE-2025-4828

Descripción: The Support Board plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the sb_file_delete function in all versions up to, and including, 3.8.0. This makes it possible for 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). An attacker can lev...

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-22

Tecnología: No especificado

Publicado el: 2025-07-09

CVE-2025-4855

Descripción: The Support Board plugin for WordPress is vulnerable to unauthorized access/modification/deletion of data due to use of hardcoded default secrets in the sb_encryption() function in all versions up to, and including, 3.8.0. This makes it possible for unauthenticated attackers to bypass authorization and execute arbitrary AJAX actions defined in the sb_ajax_execute() function. An attacker can use...

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-639

Tecnología: No especificado

Publicado el: 2025-07-09

CVE-2025-7211

Descripción: A vulnerability was found in code-projects LifeStyle Store 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cart_add.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: 2025-07-09

CVE-2025-4606

Descripción: The Sala - Startup & SaaS WordPress Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.1.4. This is due to the theme not properly validating a user's identity prior to updating their details like password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, ...

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-620

Tecnología: No especificado

Publicado el: 2025-07-09

CVE-2025-7217

Descripción: A vulnerability has been found in Campcodes Payroll Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.php?action=save_position. 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: 2025-07-09

CVE-2025-7218

Descripción: A vulnerability was found in Campcodes Payroll Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /ajax.php?action=delete_position. The manipulation of the argument 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: 2025-07-09

CVE-2025-7219

Descripción: A vulnerability was found in Campcodes Payroll Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /ajax.php?action=delete_allowances. The manipulation of the argument ID 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: 2025-07-09

CVE-2025-7220

Descripción: A vulnerability was found in Campcodes Payroll Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=save_deductions. The manipulation of the argument ID 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: 2025-07-09

CVE-2025-7401

Descripción: The Premium Age Verification / Restriction for WordPress plugin for WordPress is vulnerable to arbitrary file read and write due to the existence of an insufficiently protected remote support functionality in remote_tunnel.php in all versions up to, and including, 3.0.2. This makes it possible for unauthenticated attackers to read from or write to arbitrary files on the affected site's server w...

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-798

Tecnología: No especificado

Publicado el: 2025-07-11

CVE-2025-5392

Descripción: The GB Forms DB plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.0.2 via the gbfdb_talk_to_front() function. This is due to the function accepting user input and then passing that through call_user_func(). This makes it possible for unauthenticated attackers to execute code on the server which can be leverage to inject backdoors or create new a...

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: 2025-07-11

CVE-2025-52950

Descripción: A Missing Authorization vulnerability in Juniper Networks Security Director allows an unauthenticated network-based attacker to read or tamper with multiple sensitive resources via the web interface.

Numerous endpoints on the Juniper Security Director appliance do not validate authorization and will deliver information to the caller that is outside their authorization level. An attacker can ac...

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-07-11

CVE-2025-6058

Descripción: The WPBookit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the image_upload_handle() function hooked via the 'add_booking_type' route in all versions up to, and including, 1.0.4. 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: 2025-07-12

CVE-2025-7467

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 /product-detail.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: 2025-07-12

CVE-2025-7469

Descripción: A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. This issue affects some unknown processing of the file /pages/product_add.php. The manipulation of the argument prod_name 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-2025-7470

Descripción: A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been classified as critical. Affected is an unknown function of the file /pages/product_add.php. The manipulation of the argument image leads to unrestricted upload. 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-284

Tecnología: No especificado

Publicado el: 2025-07-12

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-2025-5393

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

Resumen del Reporte

CVEs analizados: 31

Promedio CVSS: 8.49

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □