CVEs más relevantes de la semana

Del 09/08/2025 al 16/08/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-8809

Descripción: A vulnerability classified as critical has been found in code-projects Online Medicine Guide 1.0. Affected is an unknown function of the file /addelidetails.php. The manipulation of the argument del 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: 2025-08-10

CVE-2025-8811

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Simple Art Gallery 1.0. Affected by this issue is some unknown functionality of the file /Admin/registration.php. The manipulation of the argument fname 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: 2025-08-10

CVE-2025-8853

Descripción: Official Document Management System developed by 2100 Technology has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to obtain any user's connection token and use it to log into the system as that user.

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-290

Tecnología: No especificado

Publicado el: 2025-08-11

CVE-2025-55150

Descripción: Stirling-PDF is a locally hosted web application that performs various operations on PDF files. Prior to version 1.1.0, when using the /api/v1/convert/html/pdf endpoint to convert HTML to PDF, the backend calls a third-party tool to process it and includes a sanitizer for security sanitization which can be bypassed and result in SSRF. This issue has been patched in version 1.1.0.

CVSS: 8.6 (HIGH)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-08-11

CVE-2025-55151

Descripción: Stirling-PDF is a locally hosted web application that performs various operations on PDF files. Prior to version 1.1.0, the "convert file to pdf" functionality (/api/v1/convert/file/pdf) uses LibreOffice's unoconvert tool for conversion, and SSRF vulnerabilities exist during the conversion process. This issue has been patched in version 1.1.0.

CVSS: 8.6 (HIGH)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-08-11

CVE-2025-55161

Descripción: Stirling-PDF is a locally hosted web application that performs various operations on PDF files. Prior to version 1.1.0, when using the /api/v1/convert/markdown/pdf endpoint to convert Markdown to PDF, the backend calls a third-party tool to process it and includes a sanitizer for security sanitization which can be bypassed and result in SSRF. This issue has been patched in version 1.1.0.

CVSS: 8.6 (HIGH)

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

Tipo: CWE-918

Tecnología: No especificado

Publicado el: 2025-08-11

CVE-2025-42950

Descripción: SAP Landscape Transformation (SLT) allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integri...

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-94

Tecnología: No especificado

Publicado el: 2025-08-12

CVE-2025-42957

Descripción: SAP S/4HANA allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integrity and availability of ...

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-94

Tecnología: No especificado

Publicado el: 2025-08-12

CVE-2025-8059

Descripción: The B Blocks plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization and improper input validation within the rgfr_registration() function in all versions up to, and including, 2.0.6. This makes it possible for unauthenticated attackers to create a new account and assign it the administrator role.

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: 2025-08-12

CVE-2025-40746

Descripción: A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.2). Affected products do not properly validate input for a backup script. This could allow an authenticated remote attacker with high privileges in the application to execute arbitrary code with 'NT Authority/SYSTEM' privileges.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-20

Tecnología: No especificado

Publicado el: 2025-08-12

CVE-2025-50165

Descripción: Untrusted pointer dereference in Microsoft Graphics Component 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-822

Tecnología: No especificado

Publicado el: 2025-08-12

CVE-2025-53766

Descripción: Heap-based buffer overflow in Windows GDI+ 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: 2025-08-12

CVE-2025-55168

Descripción: WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. Prior to version 3.4.8, a SQL Injection vulnerability was identified in the /html/saude/aplicar_medicamento.php endpoint, specifically in the id_fichamedica parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and avai...

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: 2025-08-12

CVE-2025-7384

Descripción: The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.3 via deserialization of untrusted input in the get_lead_detail function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in the Contact Form 7 plugin, which is likely to...

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: 2025-08-13

CVE-2025-8760

Descripción: A vulnerability was identified in INSTAR 2K+ and 4K 3.11.1 Build 1124. This affects the function base64_decode of the component fcgi_server. The manipulation of the argument Authorization leads to buffer overflow. It is possible to initiate the attack remotely.

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: 2025-08-13

CVE-2025-8913

Descripción: Organization Portal System developed by WellChoose has a Local File Inclusion vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server.

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-98

Tecnología: No especificado

Publicado el: 2025-08-13

CVE-2025-51452

Descripción: In TOTOLINK A7000R firmware 9.1.0u.6115_B20201022, an attacker can bypass login by sending a specific request through formLoginAuth.htm.

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: NVD-CWE-noinfo

Tecnología: No especificado

Publicado el: 2025-08-13

CVE-2025-51451

Descripción: In TOTOLINK EX1200T firmware 4.1.2cu.5215, an attacker can bypass login by sending a specific request through formLoginAuth.htm.

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: NVD-CWE-noinfo

Tecnología: No especificado

Publicado el: 2025-08-13

CVE-2025-8921

Descripción: A vulnerability has been found in code-projects Job Diary 1.0. Affected by this issue is some unknown functionality of the file /user-apply.php. The manipulation of the argument job_title 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: 2025-08-13

CVE-2025-8922

Descripción: A vulnerability was found in code-projects Job Diary 1.0. This affects an unknown part of the file /admin-inbox.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: 2025-08-13

CVE-2025-8923

Descripción: A vulnerability was determined in code-projects Job Diary 1.0. This vulnerability affects unknown code of the file /edit-details.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: 2025-08-13

CVE-2025-8924

Descripción: A vulnerability was identified in Campcodes Online Water Billing System 1.0. This issue affects some unknown processing of the file /viewbill.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: 2025-08-13

CVE-2025-8925

Descripción: A vulnerability has been found in itsourcecode Sports Management System 1.0. Affected is an unknown function of the file /Admin/match.php. The manipulation of the argument code 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: 2025-08-13

CVE-2025-8926

Descripción: A vulnerability was found in SourceCodester COVID 19 Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /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: 2025-08-13

CVE-2011-10018

Descripción: myBB version 1.6.4 was distributed with an unauthorized backdoor embedded in the source code. The backdoor allowed remote attackers to execute arbitrary PHP code by injecting payloads into a specially crafted collapsed cookie. This vulnerability was introduced during packaging and was not part of the intended application logic. Exploitation requires no authentication and results in full comprom...

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: 2025-08-13

CVE-2025-8932

Descripción: A vulnerability was determined in 1000 Projects Sales Management System 1.0. This vulnerability affects unknown code of the file /superstore/admin/sales.php. The manipulation of the argument ssalescat 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: 2025-08-14

CVE-2025-8935

Descripción: A vulnerability was found in 1000 Projects Sales Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /superstore/custcmp.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: 2025-08-14

CVE-2025-8936

Descripción: A vulnerability was determined in 1000 Projects Sales Management System 1.0. Affected by this issue is some unknown functionality of the file /superstore/dist/dordupdate.php. The manipulation of the argument select2 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: 2025-08-14

CVE-2025-8946

Descripción: A vulnerability has been found in projectworlds Online Notes Sharing Platform 1.0. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument User 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: 2025-08-14

CVE-2025-8947

Descripción: A vulnerability was found in projectworlds Visitor Management System 1.0. This issue affects some unknown processing of the file /query_data.php. The manipulation of the argument dateF/dateP 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: 2025-08-14

CVE-2025-8948

Descripción: A vulnerability was determined in projectworlds Visitor Management System 1.0. Affected is an unknown function of the file /front.php. The manipulation of the argument rid 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: 2025-08-14

CVE-2025-8950

Descripción: A vulnerability was identified in Campcodes Online Recruitment Management System 1.0. This issue affects some unknown processing of the file /Recruitment/index.php?page=view_vacancy. 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: 2025-08-14

CVE-2025-8951

Descripción: A vulnerability has been found in PHPGurukul Teachers Record Management System 2.1. Affected is an unknown function of the file /admin/search.php. The manipulation of the argument searchdata 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: 2025-08-14

CVE-2025-8952

Descripción: A vulnerability was found in Campcodes Online Flight Booking Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=login of the component Login. 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: 2025-08-14

CVE-2025-8954

Descripción: A vulnerability was identified in PHPGurukul Hospital Management System 4.0. This affects an unknown part of the file /admin/doctor-specilization.php. The manipulation of the argument doctorspecilization 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: 2025-08-14

CVE-2025-8955

Descripción: A vulnerability has been found in PHPGurukul Hospital Management System 4.0. This vulnerability affects unknown code of the file /admin/edit-doctor.php. The manipulation of the argument docfees 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: 2025-08-14

CVE-2025-8957

Descripción: A vulnerability was determined in Campcodes Online Flight Booking Management System 1.0. Affected is an unknown function of the file /flights.php. The manipulation of the argument departure_airport_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: 2025-08-14

CVE-2025-8960

Descripción: A vulnerability has been found in Campcodes Online Flight Booking Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/save_airlines.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: 2025-08-14

CVE-2025-6679

Descripción: The Bit Form builder plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in all versions up to, and including, 2.20.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. For this to be exploitable, the PRO version needs to be installed and activat...

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: 2025-08-15

CVE-2025-7778

Descripción: The Icons Factory plugin for WordPress is vulnerable to Arbitrary File Deletion due to insufficient authorization and improper path validation within the delete_files() function in all versions up to, and including, 1.6.12. This makes it possible for unauthenticated attackers to to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is delete...

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-285

Tecnología: No especificado

Publicado el: 2025-08-15

CVE-2025-7441

Descripción: The StoryChief plugin for WordPress is vulnerable to arbitrary file uploads in all versions up to, and including, 1.0.42. This vulnerability occurs through the /wp-json/storychief/webhook REST-API endpoint that does not have sufficient filetype validation. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code exec...

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: 2025-08-16

CVE-2025-8898

Descripción: The Taxi Booking Manager for Woocommerce | E-cab plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.3.0. This is due to the plugin not properly validating a user's capabilities prior to updating a plugin setting or their identity prior to updating their details like email address. This makes it possible for unauthenticated att...

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: 2025-08-16

Resumen del Reporte

CVEs analizados: 42

Promedio CVSS: 8.45

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯