CVEs más relevantes de la semana

Del 12/08/2025 al 19/08/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-55167

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/funcionario/dependente_remover.php endpoint, specifically in the id_dependente parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and ...

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-2025-50165

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-2025-8949

Descripción: A vulnerability was identified in D-Link DIR-825 2.10. Affected by this vulnerability is the function get_ping_app_stat of the file ping_response.cgi of the component httpd. The manipulation of the argument ping_ipaddr leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products ...

CVSS: 7.2 (HIGH)

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

Tipo: CWE-119

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-2025-8953

Descripción: A vulnerability was determined in SourceCodester COVID 19 Testing Management System 1.0. Affected by this issue is some unknown functionality of the file /check_availability.php. The manipulation of the argument employeeid 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-2025-8954

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-2025-8966

Descripción: A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/operations/tax.php. The manipulation of the argument tname 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-2025-8967

Descripción: A vulnerability was determined in itsourcecode Online Tour and Travel Management System 1.0. Affected is an unknown function of the file /admin/operations/packages.php. The manipulation of the argument pname 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-2025-8968

Descripción: A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/disapprove_user.php. 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: 2025-08-14

CVE-2025-8969

Descripción: A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/approve_user.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-2025-8970

Descripción: A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This affects an unknown part of the file /admin/operations/booking.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: 2025-08-14

CVE-2025-8971

Descripción: A vulnerability was determined in itsourcecode Online Tour and Travel Management System 1.0. This vulnerability affects unknown code of the file /admin/operations/travellers.php. The manipulation of the argument val-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: 2025-08-14

CVE-2025-8972

Descripción: A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/page-login.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: 2025-08-14

CVE-2025-8981

Descripción: A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This affects an unknown part of the file /admin/operations/payment.php. The manipulation of the argument payment_type 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-2025-8982

Descripción: A vulnerability was determined in itsourcecode Online Tour and Travel Management System 1.0. This vulnerability affects unknown code of the file /admin/operations/currency.php. The manipulation of the argument curr_code 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-2025-8983

Descripción: A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/operations/expense.php. The manipulation of the argument expense_for 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-2025-8984

Descripción: A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Affected is an unknown function of the file /admin/operations/expense_category.php. The manipulation of the argument expense_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: 2025-08-14

CVE-2025-8985

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 /profile.php. The manipulation of the argument mobilenumber 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 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: 2025-08-14

CVE-2025-8986

Descripción: A vulnerability was determined in SourceCodester COVID 19 Testing Management System 1.0. Affected by this issue is some unknown functionality of the file /search-report-result.php. The manipulation of the argument serachdata 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-2025-8987

Descripción: A vulnerability was identified in SourceCodester COVID 19 Testing Management System 1.0. This affects an unknown part of the file /test-details.php. The manipulation of the argument remark 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-2025-8988

Descripción: A vulnerability has been found in SourceCodester COVID 19 Testing Management System 1.0. This vulnerability affects unknown code of the file /bwdates-report-result.php. The manipulation of the argument fromdate 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-2025-8989

Descripción: A vulnerability was found in SourceCodester COVID 19 Testing Management System 1.0. This issue affects some unknown processing of the file /edit-phlebotomist.php. The manipulation of the argument mobilenumber leads to sql injection. The attack may be initiated 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: 2025-08-15

CVE-2025-8993

Descripción: A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. This affects an unknown part of the file /admin/expense_report.php. The manipulation of the argument from_date 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: 2025-08-15

CVE-2025-9008

Descripción: A vulnerability was identified in itsourcecode Online Tour and Travel Management System 1.0. This issue affects some unknown processing of the file /admin/sms_setting.php. The manipulation of the argument uname 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: 2025-08-15

CVE-2025-9009

Descripción: A vulnerability has been found in itsourcecode Online Tour and Travel Management System 1.0. Affected is an unknown function of the file /admin/email_setup.php. The manipulation of the argument 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: 2025-08-15

CVE-2025-9010

Descripción: A vulnerability was found in itsourcecode Online Tour and Travel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/booking_report.php. The manipulation of the argument from_date 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: 2025-08-15

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-2025-9026

Descripción: A vulnerability was identified in D-Link DIR-860L 2.04.B04. This affects the function ssdpcgi_main of the file htdocs/cgibin of the component Simple Service Discovery Protocol. The manipulation leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer su...

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-77

Tecnología: No especificado

Publicado el: 2025-08-15

CVE-2025-9047

Descripción: A vulnerability has been found in projectworlds Visitor Management System 1.0. Affected is an unknown function of the file /visitor_out.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: 2025-08-15

CVE-2025-9050

Descripción: A vulnerability was found in projectworlds Travel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /addcategory.php. The manipulation of the argument t1 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: 2025-08-15

CVE-2025-9051

Descripción: A vulnerability was determined in projectworlds Travel Management System 1.0. Affected by this issue is some unknown functionality of the file /updatecategory.php. The manipulation of the argument t1 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: 2025-08-15

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

CVE-2025-6758

Descripción: The Real Spaces - WordPress Properties Directory Theme theme for WordPress is vulnerable to privilege escalation via the 'imic_agent_register' function in all versions up to, and including, 3.6. This is due to a lack of restriction in the registration role. This makes it possible for unauthenticated attackers to arbitrarily choose their role, including the Administrator role, during user regist...

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-269

Tecnología: No especificado

Publicado el: 2025-08-19

CVE-2025-8723

Descripción: The Cloudflare Image Resizing plugin for WordPress is vulnerable to Remote Code Execution due to missing authentication and insufficient sanitization within its hook_rest_pre_dispatch() method in all versions up to, and including, 1.5.6. This makes it possible for unauthenticated attackers to inject arbitrary PHP into the codebase, achieving remote code execution.

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: 2025-08-19

Resumen del Reporte

CVEs analizados: 61

Promedio CVSS: 7.95

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat