CVEs más relevantes de la semana

Del 05/07/2025 al 12/07/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-41672

Descripción: A remote unauthenticated attacker may use default certificates to generate JWT Tokens and gain full access to the tool and all connected devices.

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-1188

Tecnología: No especificado

Publicado el: 2025-07-07

CVE-2025-7119

Descripción: A vulnerability has been found in Campcodes Complaint Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /users/index.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: 2025-07-07

CVE-2025-7120

Descripción: A vulnerability was found in Campcodes Complaint Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /users/check_availability.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: 2025-07-07

CVE-2025-3626

Descripción: A remote attacker with administrator account can gain full control of the device due to improper neutralization of special elements used in an OS Command ('OS Command Injection') while uploading a config file via webUI.

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-78

Tecnología: No especificado

Publicado el: 2025-07-07

CVE-2025-7122

Descripción: A vulnerability was found in Campcodes Complaint Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/index.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: 2025-07-07

CVE-2025-7128

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=calculate_payroll. 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: 2025-07-07

CVE-2025-7129

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_employee_attendance_single. 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: 2025-07-07

CVE-2025-7130

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_payroll. 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: 2025-07-07

CVE-2025-7131

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_employee_attendance. The manipulation of the argument employee_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: 2025-07-07

CVE-2025-7132

Descripción: A vulnerability was found in Campcodes Payroll Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ajax.php?action=save_payroll. 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: 2025-07-07

CVE-2025-7134

Descripción: A vulnerability classified as critical was found in Campcodes Online Recruitment Management System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=delete_application. 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: 2025-07-07

CVE-2025-7135

Descripción: A vulnerability, which was classified as critical, has been found in Campcodes Online Recruitment Management System 1.0. This issue affects some unknown processing of the file /admin/ajax.php?action=save_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: 2025-07-07

CVE-2025-53527

Descripción: WeGIA is a web manager for charitable institutions. A Time-Based Blind SQL Injection vulnerability was discovered in the almox parameter of the /controle/relatorio_geracao.php endpoint. This issue allows attacker to inject arbitrary SQL queries, potentially leading to unauthorized data access or further exploitation depending on database configuration. This vulnerability is fixed in 3.4.1.

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: 2025-07-07

CVE-2025-7136

Descripción: A vulnerability, which was classified as critical, was found in Campcodes Online Recruitment Management System 1.0. Affected is an unknown function of the file /admin/view_vacancy.php. 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: 2025-07-07

CVE-2025-7147

Descripción: A vulnerability has been found in CodeAstro Patient Record Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument uname 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: 2025-07-07

CVE-2025-42963

Descripción: A critical vulnerability in SAP NetWeaver Application server for Java Log Viewer enables authenticated administrator users to exploit unsafe Java object deserialization. Successful exploitation can lead to full operating system compromise, granting attackers complete control over the affected system. This results in a severe impact on the confidentiality, integrity, and availability of the appl...

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-42964

Descripción: SAP NetWeaver Enterprise Portal Administration is vulnerable when a privileged user can upload untrusted or malicious content which, when deserialized, could potentially lead to a compromise of confidentiality, integrity, and availability of the host system.

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-42966

Descripción: SAP NetWeaver XML Data Archiving Service allows an authenticated attacker with administrative privileges to exploit an insecure Java deserialization vulnerability by sending a specially crafted serialized Java object. This could lead to high impact on confidentiality, integrity, and availability of the application.

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-42967

Descripción: SAP S/4HANA and SAP SCM Characteristic Propagation has remote code execution vulnerability. This allows an attacker with user level privileges to create a new report with his own code potentially gaining full control of the affected SAP system causing high impact on confidentiality, integrity, and availability of the application.

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: 2025-07-08

CVE-2025-42980

Descripción: SAP NetWeaver Enterprise Portal Federated Portal Network is vulnerable when a privileged user can upload untrusted or malicious content which, when deserialized, could potentially lead to a compromise of confidentiality, integrity, and availability of the host system.

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-502

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-7155

Descripción: A vulnerability, which was classified as critical, was found in PHPGurukul Online Notes Sharing System 1.0. This affects an unknown part of the file /Dashboard of the component Cookie Handler. The manipulation of the argument sessionid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The original researcher dis...

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-2025-7157

Descripción: A vulnerability was found in code-projects Online Note Sharing 1.0. It has been classified as critical. Affected is an unknown function of the file /login.php. The manipulation of the argument username/password 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-2025-7160

Descripción: A vulnerability classified as critical has been found in PHPGurukul Zoo Management System 2.1. This affects an unknown part of the file /admin/index.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: 2025-07-08

CVE-2025-7164

Descripción: A vulnerability has been found in PHPGurukul/Campcodes Cyber Cafe Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /index.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: 2025-07-08

CVE-2025-7165

Descripción: A vulnerability was found in PHPGurukul/Campcodes Cyber Cafe Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /forgot-password.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: 2025-07-08

CVE-2025-25270

Descripción: An unauthenticated remote attacker can alter the device configuration in a way to get remote code execution as root with specific configurations.

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-913

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-7168

Descripción: A vulnerability was found in code-projects Crime Reporting System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /userlogin.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: 2025-07-08

CVE-2025-7169

Descripción: A vulnerability classified as critical has been found in code-projects Crime Reporting System 1.0. Affected is an unknown function of the file /complainer_page.php. The manipulation of the argument location 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-2025-7170

Descripción: A vulnerability classified as critical was found in code-projects Crime Reporting System 1.0. Affected by this vulnerability is an unknown functionality of the file /registration.php. The manipulation of the argument 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: 2025-07-08

CVE-2025-7171

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Crime Reporting System 1.0. Affected by this issue is some unknown functionality of the file /policelogin.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: 2025-07-08

CVE-2025-7172

Descripción: A vulnerability, which was classified as critical, was found in code-projects Crime Reporting System 1.0. This affects an unknown part of the file /headlogin.php. The manipulation of the argument email 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-2025-7173

Descripción: A vulnerability has been found in code-projects Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file /add-student.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-2025-40736

Descripción: A vulnerability has been identified in SINEC NMS (All versions < V4.0). The affected application exposes an endpoint that allows an unauthorized modification of administrative credentials. This could allow an unauthenticated attacker to reset the superadmin password and gain full control of the application (ZDI-CAN-26569).

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-306

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-7174

Descripción: A vulnerability was found in code-projects Library System 1.0 and classified as critical. This issue affects some unknown processing of the file /teacher-issue-book.php. The manipulation of the argument idn 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-2025-7176

Descripción: A vulnerability was found in PHPGurukul Hospital Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file view-medhistory.php. The manipulation of the argument viewid 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: 2025-07-08

CVE-2025-21450

Descripción: Cryptographic issue occurs due to use of insecure connection method while downloading.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-287

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-7178

Descripción: A vulnerability classified as critical has been found in code-projects Food Distributor Site 1.0. This affects an unknown part of the file /admin/login.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: 2025-07-08

CVE-2025-7179

Descripción: A vulnerability classified as critical was found in code-projects Library System 1.0. This vulnerability affects unknown code of the file /add-teacher.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-2025-7180

Descripción: A vulnerability, which was classified as critical, has been found in code-projects Staff Audit System 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument User 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-2025-7181

Descripción: A vulnerability, which was classified as critical, was found in code-projects Staff Audit System 1.0. Affected is an unknown function of the file /test.php. The manipulation of the argument uploadedfile 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: 6.3 (MEDIUM)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-07-08

CVE-2025-7183

Descripción: A vulnerability was found in Campcodes Sales and Inventory System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pages/customer_account.php. The manipulation of the argument Customer 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-2025-7184

Descripción: A vulnerability was found in code-projects Library System 1.0. It has been classified as critical. This affects an unknown part of the file /user/teacher/books.php. The manipulation of the argument Search 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-2025-7185

Descripción: A vulnerability was found in code-projects Library System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /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: 2025-07-08

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-2020-36847

Descripción: The Simple-File-List Plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 4.2.2 via the rename function which can be used to rename uploaded PHP code with a png extension to use a php extension. This allows unauthenticated attackers to execute 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-434

Tecnología: No especificado

Publicado el: 2025-07-12

Resumen del Reporte

CVEs analizados: 66

Promedio CVSS: 8.08

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat