CVEs más relevantes de la semana

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

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-54261

Descripción: ColdFusion versions 2025.3, 2023.15, 2021.21 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary code execution by an attacker. Scope is changed.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-55232

Descripción: Deserialization of untrusted data in Microsoft High Performance Compute Pack (HPC) 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-502

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-55234

Descripción: SMB Server might be susceptible to relay attacks depending on the configuration. An attacker who successfully exploited these vulnerabilities could perform relay attacks and make the users subject to elevation of privilege attacks. The SMB Server already supports mechanisms for hardening against relay attacks:

SMB Server signing SMB Server Extended Protection for Authentication (EPA)

Microsof...

CVSS: 8.8 (HIGH)

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

Tipo: CWE-287

Tecnología: No especificado

Publicado el: 2025-09-09

CVE-2025-8570

Descripción: The BeyondCart Connector plugin for WordPress is vulnerable to Privilege Escalation due to improper JWT secret management and authorization within the determine_current_user filter in versions 1.4.2 through 2.1.0. This makes it possible for unauthenticated attackers to craft valid tokens and assume any user's identity.

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: 2025-09-11

CVE-2025-40687

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'mobilenumber', 'teamleadname' and 'teammember' parameters in the endpoint '/ofrs/admin/add-team.php'.

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: 2025-09-11

CVE-2025-40689

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'remark', 'status' and 'requestid' parameters in the endpoint '/ofrs/admin/request-details.php'.

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: 2025-09-11

CVE-2025-40690

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via 'teamid' parameter in the endpoint '/ofrs/admin/edit-team.php'.

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: 2025-09-11

CVE-2025-40691

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'todate' parameter in the endpoint '/ofrs/admin/bwdates-report-result.php'.

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: 2025-09-11

CVE-2025-40692

Descripción: SQL Injection in Online Fire Reporting System v1.2 by PHPGurukul. This vulnerability allows an attacker to retrieve, create, update and delete database via

'requestid' parameter in the endpoint '/ofrs/details.php'.

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: 2025-09-11

CVE-2025-10264

Descripción: Certain models of NVR developed by Digiever has an Exposure of Sensitive Information vulnerability, allowing unauthenticated remoter attackers to access the system configuration file and obtain plaintext credentials of the NVR and its connected cameras.

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-497

Tecnología: No especificado

Publicado el: 2025-09-12

CVE-2025-10266

Descripción: NUP Pro developed by NewType Infortech has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

CVSS: 9.8 (CRITICAL)

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

Tipo: CWE-89

Tecnología: No especificado

Publicado el: 2025-09-12

CVE-2025-10392

Descripción: A vulnerability was detected in Mercury KM08-708H GiGA WiFi Wave2 1.1.14. This affects an unknown function of the component HTTP Header Handler. The manipulation of the argument Host results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.

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: 2025-09-14

CVE-2025-10452

Descripción: Statistical Database System developed by Gotac has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents with high-level privileges.

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: 2025-09-15

CVE-2025-10432

Descripción: A vulnerability was found in Tenda AC1206 15.03.06.23. This vulnerability affects the function check_param_changed of the file /goform/AdvSetMacMtuWa of the component HTTP Request Handler. Performing manipulation of the argument wanMTU results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used.

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: 2025-09-15

CVE-2025-4688

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BGS Interactive SINAV.LINK Exam Result Module allows SQL Injection.This issue affects SINAV.LINK Exam Result Module: before 1.2.

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: 2025-09-16

CVE-2025-7743

Descripción: Cleartext Transmission of Sensitive Information vulnerability in Dolusoft Omaspot allows Interception, Privilege Escalation.This issue affects Omaspot: before 12.09.2025.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-319

Tecnología: No especificado

Publicado el: 2025-09-16

CVE-2025-7744

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Dolusoft Omaspot allows SQL Injection.This issue affects Omaspot: before 12.09.2025.

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: 2025-09-16

CVE-2025-8276

Descripción: Improper Encoding or Escaping of Output, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'), Improper Control of Generation of Code ('Code Injection') vulnerability in Patika Global Technologies HumanSuite allows Input Data Manipulation, Format String Injection, Re...

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-16

CVE-2024-13149

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 200 - Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Arma Store Armalife allows SQL Injection.This issue affects Armalife: through 20250916.

NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when ne...

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: 2025-09-16

Resumen del Reporte

CVEs analizados: 19

Promedio CVSS: 9.72

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat