CVEs más relevantes de la semana

Del 07/02/2026 al 14/02/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2026-2087

Descripción: A flaw has been found in SourceCodester Online Class Record System 1.0. Affected by this issue is some unknown functionality of the file /admin/login.php. This manipulation of the argument user_email causes sql injection. The attack may be initiated remotely. The exploit has been published 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: 2026-02-07

CVE-2026-2088

Descripción: A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown part of the file /admin/accepted-appointment.php. Such manipulation of the argument delid 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: 2026-02-07

CVE-2026-2089

Descripción: A vulnerability was found in SourceCodester Online Class Record System 1.0. This vulnerability affects unknown code of the file /admin/subject/controller.php. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could 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: 2026-02-07

CVE-2026-2090

Descripción: A vulnerability was determined in SourceCodester Online Class Record System 1.0. This issue affects some unknown processing of the file /admin/message/search.php. Executing a manipulation of the argument term can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.

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: 2026-02-07

CVE-2026-25560

Descripción: WeKan versions prior to 8.19 contain an LDAP filter injection vulnerability in LDAP authentication. User-supplied username input is incorporated into LDAP search filters and DN-related values without adequate escaping, allowing an attacker to manipulate LDAP queries during authentication.

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-90

Tecnología: No especificado

Publicado el: 2026-02-07

CVE-2026-2114

Descripción: A vulnerability was detected in itsourcecode Society Management System 1.0. This vulnerability affects unknown code of the file /admin/edit_admin.php. The manipulation of the argument admin_id results in sql injection. The attack may be performed from remote. The exploit is now 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: 2026-02-07

CVE-2026-2115

Descripción: A flaw has been found in itsourcecode Society Management System 1.0. This issue affects some unknown processing of the file /admin/delete_expenses.php. This manipulation of the argument expenses_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been published 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: 2026-02-07

CVE-2026-2116

Descripción: A vulnerability has been found in itsourcecode Society Management System 1.0. Impacted is an unknown function of the file /admin/edit_expenses.php. Such manipulation of the argument expenses_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: 2026-02-08

CVE-2026-2117

Descripción: A vulnerability was found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/edit_activity.php. Performing a manipulation of the argument activity_id results in sql injection. The attack can be initiated remotely. The exploit has been made public and could 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: 2026-02-08

CVE-2025-15027

Descripción: The JAY Login & Register plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.6.03. This is due to the plugin allowing a user to update arbitrary user meta through the 'jay_login_register_ajax_create_final_user' function. This makes it possible for unauthenticated attackers to elevate their privileges to that of an administrator.

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: 2026-02-08

CVE-2026-2132

Descripción: A security flaw has been discovered in code-projects Online Music Site 1.0. This issue affects some unknown processing of the file /Administrator/PHP/AdminUpdateCategory.php. The manipulation of the argument txtcat results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.

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: 2026-02-08

CVE-2026-2133

Descripción: A weakness has been identified in code-projects Online Music Site 1.0. Impacted is an unknown function of the file /Administrator/PHP/AdminUpdateCategory.php. This manipulation of the argument txtimage causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.

CVSS: 7.3 (HIGH)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2026-02-08

CVE-2026-2136

Descripción: A flaw has been found in projectworlds Online Food Ordering System 1.0. This affects an unknown function of the file /view-ticket.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published 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: 2026-02-08

CVE-2026-2158

Descripción: A vulnerability was detected in code-projects Student Web Portal 1.0. This impacts an unknown function of the file /check_user.php. Performing a manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely.

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: 2026-02-08

CVE-2026-2161

Descripción: A vulnerability was found in itsourcecode Directory Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/forget-password.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been made public and could 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: 2026-02-08

CVE-2026-2166

Descripción: A security vulnerability has been detected in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /login/index.php of the component Login. The manipulation of the argument username/password leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly 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: 2026-02-08

CVE-2026-2171

Descripción: A vulnerability was found in code-projects Online Student Management System 1.0. Affected is an unknown function of the file accounts.php of the component Login. Performing a manipulation of the argument username/password results in sql injection. The attack can be initiated remotely. The exploit has been made public and could 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: 2026-02-08

CVE-2026-2172

Descripción: A vulnerability was determined in code-projects Online Application System for Admission 1.0. Affected by this vulnerability is an unknown functionality of the file enrollment/index.php of the component Login Endpoint. Executing a manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.

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: 2026-02-08

CVE-2026-2173

Descripción: A vulnerability was identified in code-projects Online Examination System 1.0. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack may be initiated remotely.

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: 2026-02-08

CVE-2026-2174

Descripción: A security flaw has been discovered in code-projects Contact Management System 1.0. This affects an unknown part of the component CRUD Endpoint. The manipulation of the argument ID results in improper authentication. The attack may be launched remotely.

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-287

Tecnología: No especificado

Publicado el: 2026-02-08

CVE-2026-2189

Descripción: A vulnerability was identified in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/report/index.php. The manipulation of the argument ay leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might 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: 2026-02-08

CVE-2026-2190

Descripción: A security flaw has been discovered in itsourcecode School Management System 1.0. This impacts an unknown function of the file /ramonsys/user/controller.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.

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: 2026-02-08

CVE-2026-2195

Descripción: A vulnerability has been found in code-projects Online Reviewer System 1.0. This vulnerability affects unknown code of the file /system/system/admins/assessments/pretest/questions-view.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out 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: 2026-02-09

CVE-2026-2196

Descripción: A vulnerability was found in code-projects Online Reviewer System 1.0. This issue affects some unknown processing of the file /system/system/admins/assessments/pretest/exam-update.php. The manipulation of the argument test_id results in sql injection. The attack may be performed from remote. The exploit has been made public and could 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: 2026-02-09

CVE-2026-2197

Descripción: A vulnerability was determined in code-projects Online Reviewer System 1.0. Impacted is an unknown function of the file /system/system/admins/assessments/pretest/exam-delete.php. This manipulation of the argument test_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.

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: 2026-02-09

CVE-2026-2198

Descripción: A vulnerability was identified in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /system/system/admins/assessments/pretest/loaddata.php. Such manipulation of the argument difficulty_id leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might 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: 2026-02-09

CVE-2026-2199

Descripción: A security flaw has been discovered in code-projects Online Reviewer System 1.0. The impacted element is an unknown function of the file /reviewer/system/system/admins/manage/users/user-delete.php. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.

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: 2026-02-09

CVE-2026-2211

Descripción: A vulnerability was determined in code-projects Online Music Site 1.0. Affected is an unknown function of the file /Administrator/PHP/AdminDeleteCategory.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.

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: 2026-02-09

CVE-2026-2212

Descripción: A vulnerability was identified in code-projects Online Music Site 1.0. Affected by this vulnerability is an unknown functionality of the file /Administrator/PHP/AdminEditCategory.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might 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: 2026-02-09

CVE-2026-2217

Descripción: A vulnerability was found in itsourcecode Event Management System 1.0. The impacted element is an unknown function of the file /admin/manage_user.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could 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: 2026-02-09

CVE-2026-2220

Descripción: A vulnerability was identified in code-projects Online Reviewer System 1.0. This impacts an unknown function of the file /system/system/admins/assessments/pretest/btn_functions.php. Such manipulation of the argument difficulty_id leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might 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: 2026-02-09

CVE-2026-2221

Descripción: A security flaw has been discovered in code-projects Online Reviewer System 1.0. Affected is an unknown function of the file /login/index.php of the component Login. Performing a manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.

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: 2026-02-09

CVE-2026-22903

Descripción: An unauthenticated remote attacker can send a crafted HTTP request containing an overly long SESSIONID cookie. This can trigger a stack buffer overflow in the modified lighttpd server, causing it to crash and potentially enabling remote code execution due to missing stack protections.

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-121

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-22904

Descripción: Improper length handling when parsing multiple cookie fields (including TRACKID) allows an unauthenticated remote attacker to send oversized cookie values and trigger a stack buffer overflow, resulting in a denial-of-service condition and possible 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-121

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-22906

Descripción: User credentials are stored using AES-ECB encryption with a hardcoded key. An unauthenticated remote attacker obtaining the configuration file can decrypt and recover plaintext usernames and passwords, especially when combined with the authentication bypass.

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-321

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-2223

Descripción: A security vulnerability has been detected in code-projects Online Reviewer System 1.0. Affected by this issue is some unknown functionality of the file /system/system/students/assessments/pretest/take/index.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly 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: 2026-02-09

CVE-2026-2234

Descripción: C&Cm@il developed by HGiga has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read and modify any user's mail content.

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-306

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-2225

Descripción: A flaw has been found in itsourcecode News Portal Project 1.0. This vulnerability affects unknown code of the file /admin/index.php of the component Administrator Login. This manipulation of the argument email causes sql injection. The attack can be initiated remotely. The exploit has been published 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: 2026-02-09

CVE-2026-24677

Descripción: FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, ecam_encoder_compress_h264 trusts server-controlled dimensions and does not validate the source buffer size, leading to an out-of-bounds read in sws_scale. This vulnerability is fixed in 3.22.0.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-416

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-24679

Descripción: FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, The URBDRC client uses server-supplied interface numbers as array indices without bounds checks, causing an out-of-bounds read in libusb_udev_select_interface. This vulnerability is fixed in 3.22.0.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-122

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-25809

Descripción: PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the code evaluation endpoint does not validate the assessment lifecycle state before allowing execution. There is no check to ensure that the assessment has started, is not expired, or the submission window is currently open.

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: 2026-02-09

CVE-2026-25810

Descripción: PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the backend/src/routes/student.submission.routes.ts verify authentication but fails to enforce object-level authorization (ownership checks).

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-862

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-25876

Descripción: PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the backend/src/routes/results.routes.ts verify authentication but fails to enforce object-level authorization (ownership checks). For example, this can be used to return all results for an assessment.

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-862

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-25875

Descripción: PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, The admin authorization middleware trusts client-controlled JWT claims (role and scope) without enforcing server-side role verification.

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-863

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-25893

Descripción: FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.2.10, an authentication bypass vulnerability in FUXA allows an unauthenticated, remote attacker to gain administrative access via the heartbeat refresh API and execute arbitrary code on the server. This issue has been patched in FUXA version 1.2.10.

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: 2026-02-09

CVE-2026-25894

Descripción: FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. An insecure default configuration in FUXA allows an unauthenticated, remote attacker to gain administrative access and execute arbitrary code on the server. This affects FUXA through version 1.2.9 when authentication is enabled, but the administrator JWT secret is not configured. This issue has been patched in FUXA versio...

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-321

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-25895

Descripción: FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. A path traversal vulnerability in FUXA allows an unauthenticated, remote attacker to write arbitrary files to arbitrary locations on the server filesystem. This affects FUXA through version 1.2.9. This issue has been patched in FUXA version 1.2.10.

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: 2026-02-09

CVE-2026-25938

Descripción: FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. From 1.2.8 through 1.2.10, an authentication bypass vulnerability in FUXA allows an unauthenticated, remote attacker to execute arbitrary code on the server when the Node-RED plugin is enabled. This has been patched in FUXA version 1.2.11.

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: 2026-02-09

CVE-2026-25939

Descripción: FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. From 1.2.8 through version 1.2.10, an authorization bypass vulnerability in the FUXA allows an unauthenticated, remote attacker to create and modify arbitrary schedulers, exposing connected ICS/SCADA environments to follow-on actions. This has been patched in FUXA version 1.2.11.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2026-02-09

CVE-2026-0488

Descripción: An authenticated attacker in SAP CRM and SAP S/4HANA (Scripting Editor) could exploit a flaw in a generic function module call and execute unauthorized critical functionalities, which includes the ability to execute an arbitrary SQL statement. This leads to a full database compromise with high impact on confidentiality, integrity, and availability.

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-862

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2026-0509

Descripción: SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated, low-privileged user to perform background Remote Function Calls without the required S_RFC authorization in certain cases. This can result in a high impact on integrity and availability, and no impact on the confidentiality of the application.

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: 2026-02-10

CVE-2026-2095

Descripción: Agentflow developed by Flowring has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to exploit a specific functionality to obtain arbitrary user authentication token and log into the system as any 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-288

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2026-2096

Descripción: Agentflow developed by Flowring has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents by using a specific functionality.

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-288

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2025-11242

Descripción: Server-Side Request Forgery (SSRF) vulnerability in Teknolist Computer Systems Software Publishing Industry and Trade Inc. Okulistik allows Server Side Request Forgery.This issue affects Okulistik: through 21102025.

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-918

Tecnología: No especificado

Publicado el: 2026-02-10

CVE-2026-21531

Descripción: Deserialization of untrusted data in Azure SDK 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: 2026-02-10

CVE-2026-1357

Descripción: The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Upload in versions up to and including 0.9.123. This is due to improper error handling in the RSA decryption process combined with a lack of path sanitization when writing uploaded files. When the plugin fails to decrypt a session key using openssl_private_decrypt(), ...

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: 2026-02-11

CVE-2025-7659

Descripción: GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that could have allowed an unauthenticated user to steal tokens and access private repositories by abusing incomplete validation in the Web IDE.

CVSS: 8.0 (HIGH)

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

Tipo: CWE-346

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2025-66277

Descripción: A link following vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to traverse the file system to unintended locations.

We have already fixed the vulnerability in the following versions: QTS 5.2.8.3350 build 20251216 and later QuTS hero h5.3.2.3354 build 20251225 and later QuTS hero h5.2.8.3350 build 202512...

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-59

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2025-8025

Descripción: Missing Authentication for Critical Function, Improper Access Control vulnerability in Dinosoft Business Solutions Dinosoft ERP allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Dinosoft ERP: from < 3.0.1 through 11022026.

NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

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-284

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2025-8668

Descripción: Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in E-Kalite Software Hardware Engineering Design and Internet Services Industry and Trade Ltd. Co. Turboard allows Reflected XSS.This issue affects Turboard: from 2025.07 through 11022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

CVSS: 9.4 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37153

Descripción: ASTPP 4.0.1 contains multiple vulnerabilities including cross-site scripting and command injection in SIP device configuration and plugin management interfaces. Attackers can exploit these flaws to inject system commands, hijack administrator sessions, and potentially execute arbitrary code with root permissions through cron task manipulation.

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-79

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37176

Descripción: Torrent 3GP Converter 1.51 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the application's registration dialog to trigger code execution and open the calculator through carefully constructed buffer overflow techniques.

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-121

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37181

Descripción: Torrent FLV Converter 1.51 Build 117 contains a stack overflow vulnerability that allows attackers to overwrite Structured Exception Handler (SEH) through a malicious registration code input. Attackers can craft a payload with specific offsets and partial SEH overwrite techniques to potentially execute arbitrary code on vulnerable Windows 32-bit systems.

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-121

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37183

Descripción: Allok RM RMVB to AVI MPEG DVD Converter 3.6.1217 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload in the License Name input field to trigger a buffer overflow and execute system commands like calc.exe.

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-121

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37184

Descripción: Allok Video Converter 4.6.1217 contains a stack overflow vulnerability in the License Name input field that allows attackers to execute arbitrary code. Attackers can craft a specially designed payload to overwrite SEH handlers and execute system commands by injecting malicious bytecode into the input field.

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-121

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2020-37186

Descripción: Chevereto 3.13.4 Core contains a remote code execution vulnerability that allows attackers to inject malicious code during database configuration installation. Attackers can manipulate the database table prefix parameter to write a PHP shell file and execute arbitrary system commands through a crafted POST request.

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: 2026-02-11

CVE-2026-26014

Descripción: Pion DTLS is a Go implementation of Datagram Transport Layer Security. Pion DTLS versions v1.0.0 through v3.0.10 and 3.1.0 use random nonce generation with AES GCM ciphers, which makes it easier for remote attackers to obtain the authentication key and spoof data by leveraging the reuse of a nonce in a session and a "forbidden attack". Upgrade to v3.0.11, v3.1.1, or later.

CVSS: 5.9 (MEDIUM)

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

Tipo: CWE-200

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2026-26021

Descripción: set-in provides the set value of nested associative structure given array of keys. A prototype pollution vulnerability exists in the the npm package set-in (>=2.0.1, < 2.0.5). Despite a previous fix that attempted to mitigate prototype pollution by checking whether user input contained a forbidden key, it is still possible to pollute Object.prototype via a crafted input using Array.prototype. T...

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-1321

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2026-20677

Descripción: A race condition was addressed with improved handling of symbolic links. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. A shortcut may be able to bypass sandbox restrictions.

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-362

Tecnología: No especificado

Publicado el: 2026-02-11

CVE-2026-1729

Descripción: The AdForest theme for WordPress is vulnerable to authentication bypass in all versions up to, and including, 6.0.12. This is due to the plugin not properly verifying a user's identity prior to authenticating them through the 'sb_login_user_with_otp_fun' function. This makes it possible for unauthenticated attackers to log in as arbitrary users, 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-306

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2025-10969

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Farktor Software E-Commerce Services Inc. E-Commerce Package allows Blind SQL Injection.This issue affects E-Commerce Package: through 27112025.

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: 2026-02-12

CVE-2025-14014

Descripción: Unrestricted Upload of File with Dangerous Type vulnerability in NTN Information Processing Services Computer Software Hardware Industry and Trade Ltd. Co. Smart Panel allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Smart Panel: before 20251215.

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: 2026-02-12

CVE-2026-26216

Descripción: Crawl4AI versions prior to 0.8.0 contain a remote code execution vulnerability in the Docker API deployment. The /crawl endpoint accepts a hooks parameter containing Python code that is executed using exec(). The __import__ builtin was included in the allowed builtins, allowing unauthenticated remote attackers to import arbitrary modules and execute system commands. Successful exploitation allo...

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-94

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2026-26218

Descripción: newbee-mall includes pre-seeded administrator accounts in its database initialization script. These accounts are provisioned with a predictable default password. Deployments that initialize or reset the database using the provided schema and fail to change the default administrative credentials may allow unauthenticated attackers to log in as an administrator and gain full administrative contro...

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: 2026-02-12

CVE-2026-26219

Descripción: newbee-mall stores and verifies user passwords using an unsalted MD5 hashing algorithm. The implementation does not incorporate per-user salts or computational cost controls, enabling attackers who obtain password hashes through database exposure, backup leakage, or other compromise vectors to rapidly recover plaintext credentials via offline attacks.

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-327

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2019-25319

Descripción: Domain Quester Pro 6.02 contains a stack overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the 'Domain Name Keywords' input field to trigger an access violation and execute a bind shell on port 9999.

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-121

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2019-25321

Descripción: FTP Navigator 8.03 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload that triggers a buffer overflow when pasted into the Custom Command textbox, enabling remote code execution and launching the calculator as proof of concept.

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-121

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2019-25327

Descripción: Prime95 version 29.8 build 6 contains a buffer overflow vulnerability in the user ID input field that allows remote attackers to execute arbitrary code. Attackers can craft a malicious payload and paste it into the PrimeNet user ID and proxy host fields to trigger a bind shell on port 3110.

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: 2026-02-12

CVE-2019-25337

Descripción: OwnCloud 8.1.8 contains a username enumeration vulnerability that allows remote attackers to discover user accounts by manipulating the share.php endpoint. Attackers can send crafted GET requests to /index.php/core/ajax/share.php with a wildcard search parameter to retrieve comprehensive user information.

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-203

Tecnología: No especificado

Publicado el: 2026-02-12

CVE-2020-37167

Descripción: ClamAV ClamBC bytecode interpreter contains a vulnerability in function name processing that allows attackers to manipulate bytecode function names. Attackers can exploit the weak input validation in function name encoding to potentially execute malicious bytecode or cause unexpected behavior in the ClamAV engine.

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: 2026-02-12

CVE-2026-1306

Descripción: The midi-Synth plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type and file extension validation in the 'export' AJAX action in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible granted the attacker can obtain a vali...

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: 2026-02-14

CVE-2025-8572

Descripción: The Truelysell Core plugin for WordPress is vulnerable to privilege escalation in versions less than, or equal to, 1.8.7. This is due to insufficient validation of the user_role parameter during user registration. This makes it possible for unauthenticated attackers to create accounts with elevated privileges, including administrator access.

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: 2026-02-14

Resumen del Reporte

CVEs analizados: 82

Promedio CVSS: 8.68

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat