CVEs más relevantes de la semana

Del 13/05/2025 al 20/05/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-30387

Descripción: Improper limitation of a pathname to a restricted directory ('path traversal') in Azure allows an unauthorized attacker to elevate privileges 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-22

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-4660

Descripción: A remote code execution vulnerability exists in the Windows agent component of SecureConnector due to improper access controls on a named pipe. The pipe is accessible to the Everyone group and does not restrict remote connections, allowing any network-based attacker to connect without authentication. By interacting with this pipe, an attacker can redirect the agent to communicate with a rogue s...

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-276

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-45746

Descripción: In ZKT ZKBio CVSecurity 6.4.1_R an unauthenticated attacker can craft JWT token using the hardcoded secret to authenticate to the service console.

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: 2025-05-13

CVE-2025-45861

Descripción: TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain a buffer overflow via the routername parameter in the formDnsv6 interface.

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-120

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-45865

Descripción: TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain a buffer overflow via the dnsaddr parameter in the formDhcpv6s interface.

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-120

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43559

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.

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-20

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43560

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-20

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43561

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass authentication mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.

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-863

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43562

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issu...

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: 2025-05-13

CVE-2025-43563

Descripción: ColdFusion versions 2025.1, 2023.13, 2021.19 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify sensitive data without proper authorization. Exploitation of this issue does not require user interaction.

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-284

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-43567

Descripción: Adobe Connect versions 12.8 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. A successful attacker can abuse this to achieve session takeover, increasi...

CVSS: 9.3 (CRITICAL)

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

Tipo: CWE-79

Tecnología: No especificado

Publicado el: 2025-05-13

CVE-2025-3917

Descripción: The □□□□SEO□□(□□□□/□□/Bing/□□□□) plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the download_remote_image_to_media_library function in all versions up to, and including, 2.0.6. 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: 2025-05-15

CVE-2025-4564

Descripción: The TicketBAI Facturas para WooCommerce plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation via the 'delpdf' action in all versions up to, and including, 3.18. This makes it possible for unauthenticated 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-co...

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: 2025-05-15

CVE-2025-4389

Descripción: The Crawlomatic Multipage Scraper Post Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the crawlomatic_generate_featured_image() function in all versions up to, and including, 2.6.8.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution poss...

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: 2025-05-17

CVE-2025-4391

Descripción: The Echo RSS Feed Post Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the echo_generate_featured_image() function in all versions up to, and including, 5.4.8.1. 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: 2025-05-17

CVE-2025-4913

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument Username 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: 2025-05-19

CVE-2025-4914

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/forgot-password.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: 2025-05-19

CVE-2025-4915

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/auto-taxi-entry-detail.php. The manipulation of the argument price 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: 2025-05-19

CVE-2025-4916

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/admin-profile.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 a...

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: 2025-05-19

CVE-2025-4917

Descripción: A vulnerability classified as critical has been found in PHPGurukul Auto Taxi Stand Management System 1.0. Affected is an unknown function of the file /admin/new-autoortaxi-entry-form.php. The manipulation of the argument drivername leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affect...

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: 2025-05-19

CVE-2025-4322

Descripción: The Motors theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 5.6.67. This is due to the theme not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user passwords, including those of administrators, and leverage that to gain access 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-620

Tecnología: No especificado

Publicado el: 2025-05-20

Resumen del Reporte

CVEs analizados: 21

Promedio CVSS: 9.01

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □