CVEs más relevantes de la semana

Del 30/12/2025 al 06/01/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-15353

Descripción: A vulnerability was detected in itsourcecode Society Management System 1.0. Impacted is the function edit_admin_query of the file /admin/edit_admin_query.php. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. 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: 2025-12-30

CVE-2025-15354

Descripción: A flaw has been found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/add_admin.php. Executing manipulation of the argument Username 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: 2025-12-30

CVE-2022-50695

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x contains a network vulnerability that allows unauthenticated attackers to send ICMP signals to arbitrary hosts through network command scripts. Attackers can abuse ping.php, traceroute.php, and dns.php to generate network flooding attacks targeting external hosts.

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-770

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2022-50790

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated vulnerability that allows remote attackers to access live radio stream information through webplay or ffmpeg scripts. Attackers can exploit the vulnerability by calling specific web scripts to disclose radio stream details without requiring 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-306

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2022-50792

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated file disclosure vulnerability that allows remote attackers to access sensitive system files. Attackers can exploit the vulnerability by manipulating the 'file' GET parameter to disclose arbitrary files on the affected device.

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: 2025-12-30

CVE-2022-50794

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated command injection vulnerability in the username parameter. Attackers can exploit index.php and login.php scripts by injecting arbitrary shell commands through the HTTP POST 'username' parameter to execute system commands.

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-78

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2022-50803

Descripción: JM-DATA ONU JF511-TV version 1.0.67 uses default credentials that allow attackers to gain unauthorized access to the device with administrative 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-1392

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2025-14998

Descripción: The Branda plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.4.24. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their...

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: 2026-01-02

CVE-2025-14996

Descripción: The AS Password Field In Default Registration Form plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.0.0. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, an...

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: 2026-01-06

CVE-2025-15001

Descripción: The FS Registration Password plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.1. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gai...

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: 2026-01-06

CVE-2020-36912

Descripción: Plexus anblick Digital Signage Management 3.1.13 contains an open redirect vulnerability in the 'PantallaLogin' script that allows attackers to manipulate the 'pagina' GET parameter. Attackers can craft malicious links that redirect users to arbitrary websites by exploiting improper input validation in the parameter.

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-601

Tecnología: No especificado

Publicado el: 2026-01-06

CVE-2020-36923

Descripción: Sony BRAVIA Digital Signage 1.7.8 contains an insecure direct object reference vulnerability that allows attackers to bypass authorization controls. Attackers can access hidden system resources like '/#/content-creation' by manipulating client-side access restrictions.

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: 2026-01-06

CVE-2020-36925

Descripción: Arteco Web Client DVR/NVR contains a session hijacking vulnerability with insufficient session ID complexity that allows remote attackers to bypass authentication. Attackers can brute force session IDs within a specific numeric range to obtain valid sessions and access live camera streams without authorization.

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-331

Tecnología: No especificado

Publicado el: 2026-01-06

Resumen del Reporte

CVEs analizados: 13

Promedio CVSS: 9.42

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯