CVEs más relevantes de la semana

Del 12/04/2025 al 19/04/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-32911

Descripción: A flaw was found in libsoup, which is vulnerable to a use-after-free memory issue not on the heap in the soup_message_headers_get_content_disposition() function. This flaw allows a malicious HTTP client to cause memory corruption in the libsoup server.

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-590

Tecnología: No especificado

Publicado el: 2025-04-15

CVE-2025-27495

Descripción: A vulnerability has been identified in TeleControl Server Basic (All versions < V3.1.2.2). The affected application is vulnerable to SQL injection through the internally used 'CreateTrace' method. This could allow an unauthenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissio...

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: 2025-04-16

CVE-2025-27539

Descripción: A vulnerability has been identified in TeleControl Server Basic (All versions < V3.1.2.2). The affected application is vulnerable to SQL injection through the internally used 'VerifyUser' method. This could allow an unauthenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permission...

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: 2025-04-16

CVE-2025-27540

Descripción: A vulnerability has been identified in TeleControl Server Basic (All versions < V3.1.2.2). The affected application is vulnerable to SQL injection through the internally used 'Authenticate' method. This could allow an unauthenticated remote attacker to bypass authorization controls, to read from and write to the application's database and execute code with "NT AUTHORITY\NetworkService" permissi...

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: 2025-04-16

CVE-2025-3278

Descripción: The UrbanGo Membership plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.0.4. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'user_register_role' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrator role.

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: 2025-04-19

Resumen del Reporte

CVEs analizados: 5

Promedio CVSS: 9.64

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat <3