CVEs más relevantes de la semana

Del 20/05/2025 al 27/05/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-4524

Descripción: The Madara – Responsive and modern WordPress theme for manga sites theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.2.2 via the 'template' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access 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: 2025-05-21

CVE-2025-4603

Descripción: The eMagicOne Store Manager for WooCommerce plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_file() function in all versions up to, and including, 1.2.5. 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 (su...

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-73

Tecnología: No especificado

Publicado el: 2025-05-24

CVE-2025-5058

Descripción: The eMagicOne Store Manager for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_image() function in all versions up to, and including, 1.2.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This is only exploitable by...

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: 2025-05-24

CVE-2025-41651

Descripción: Due to missing authentication on a critical function of the devices an unauthenticated remote attacker can execute arbitrary commands, potentially enabling unauthorized upload or download of configuration files and leading to full system compromise.

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: 2025-05-27

CVE-2025-41652

Descripción: The devices are vulnerable to an authentication bypass due to flaws in the authorization mechanism. An unauthenticated remote attacker could exploit this weakness by performing brute-force attacks to guess valid credentials or by using MD5 collision techniques to forge authentication hashes, potentially compromising the 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-656

Tecnología: No especificado

Publicado el: 2025-05-27

Resumen del Reporte

CVEs analizados: 5

Promedio CVSS: 9.66

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯