

CVEs más relevantes de la semana

Del 15/11/2025 al 22/11/2025

Porque el primer paso para defender es conocer las amenazas.



CVE-2025-13201

Descripción: A vulnerability was identified in code-projects Simple Cafe Ordering System 1.0. Affected by this issue is some unknown functionality of the file /login.php. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. 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: 2025-11-15



CVE-2025-13203

Descripción: A weakness has been identified in code-projects Simple Cafe Ordering System 1.0. This vulnerability affects unknown code of the file /addmem.php. Executing manipulation of the argument studentnum can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.

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: 2025-11-15



CVE-2025-13210

Descripción: A security vulnerability has been detected in itsourcecode Inventory Management System 1.0. This impacts an unknown function of the file /admin/products/index.php?view=add. Such manipulation of the argument PROMODEL leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.

CVSS: 4.7 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-15



CVE-2025-13233

Descripción: A vulnerability has been found in itsourcecode Inventory Management System 1.0. The affected element is an unknown function of the file /index.php?q=single-item. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. 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: 2025-11-16



CVE-2025-13234

Descripción: A vulnerability was found in itsourcecode Inventory Management System 1.0. The impacted element is an unknown function of the file /index.php?q=product. Performing manipulation of the argument PROID results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-16



CVE-2025-13235

Descripción: A vulnerability was determined in itsourcecode Inventory Management System 1.0. This affects an unknown function of the file /admin/login.php. Executing manipulation of the argument user_email can lead to sql injection. It is possible to launch 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: 2025-11-16



CVE-2025-13236

Descripción: A vulnerability was identified in itsourcecode Inventory Management System 1.0. This impacts an unknown function of the file /admin/products/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-16



CVE-2025-13237

Descripción: A security flaw has been discovered in itsourcecode Inventory Management System 1.0. Affected is an unknown function of the file /LogSignModal.PHP. The manipulation of the argument U_USERNAME results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.

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: 2025-11-16



CVE-2025-13240

Descripción: A vulnerability was detected in code-projects Student Information System 2.0. This affects an unknown part of the file /searchquery.php. Performing manipulation of the argument s results in sql injection. Remote exploitation of the attack is possible. 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: 2025-11-16



CVE-2025-13241

Descripción: A flaw has been found in code-projects Student Information System 2.0. This vulnerability affects unknown code of the file /index.php. Executing manipulation of the argument Username can lead to sql injection. The attack can be executed 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: 2025-11-16



CVE-2025-13242

Descripción: A vulnerability has been found in code-projects Student Information System 2.0. This issue affects some unknown processing of the file /register.php. The manipulation 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: 2025-11-16



CVE-2025-13247

Descripción: A security flaw has been discovered in PHPGurukul Tourism Management System 1.0. The affected element is an unknown function of the file /admin/user-bookings.php. The manipulation of the argument uid results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.

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: 2025-11-16



CVE-2025-13248

Descripción: A weakness has been identified in SourceCodester Patients Waiting Area Queue Management System 1.0. The impacted element is an unknown function of the file /php/api_patient_schedule.php. This manipulation of the argument appointmentID causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.

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: 2025-11-16



CVE-2025-13257

Descripción: A security vulnerability has been detected in itsourcecode Inventory Management System 1.0. The affected element is an unknown function of the file /admin/user/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack can be initiated 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: 2025-11-17



CVE-2025-13284

Descripción: ThinPLUS developed by ThinPLUS has an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the server.

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: 2025-11-17



CVE-2025-13267

Descripción: A vulnerability was detected in SourceCodester Dental Clinic Appointment Reservation System 1.0. Impacted is an unknown function of the file /success.php. Performing manipulation of the argument username/password results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-17



CVE-2025-13271

Descripción: A vulnerability was determined in Campcodes School Fees Payment Management System 1.0. This impacts an unknown function of the file /ajax.php?action=login. This manipulation of the argument Username causes sql injection. Remote exploitation of the attack is possible. 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: 2025-11-17



CVE-2025-13272

Descripción: A vulnerability was identified in Campcodes School Fees Payment Management System 1.0. Affected is an unknown function of the file /manage_course.php. Such manipulation of the argument 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: 2025-11-17



CVE-2025-13277

Descripción: A flaw has been found in code-projects Nero Social Networking Site 1.0. This issue affects some unknown processing of the file /friendsphoto.php. This manipulation of the argument ID 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: 2025-11-17



CVE-2025-13280

Descripción: A vulnerability was determined in CodeAstro Simple Inventory System 1.0. The impacted element is an unknown function of the file /index.php of the component Login. Executing manipulation of the argument Username can lead to sql injection. The attack may 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: 2025-11-17



CVE-2025-13285

Descripción: A vulnerability was identified in itsourcecode Online Voting System 1.0. The affected element is an unknown function of the file /login.php. Such manipulation of the argument Username leads to sql injection. The attack may be launched 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: 2025-11-17



CVE-2025-13291

Descripción: A vulnerability was found in Campcodes Supplier Management System 1.0. This affects an unknown part of the file /manufacturer/confirm_order.php. Performing manipulation of the argument 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: 2025-11-17



CVE-2025-13297

Descripción: A security vulnerability has been detected in itsourcecode Web-Based Internet Laboratory Management System 1.0. The impacted element is an unknown function of the file /course/controller.php. Such manipulation leads to sql injection. The attack can be executed 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: 2025-11-17



CVE-2025-13298

Descripción: A vulnerability was detected in itsourcecode Web-Based Internet Laboratory Management System 1.0. This affects an unknown function of the file /enrollment/controller.php. Performing manipulation results in sql injection. The attack is possible to be carried out 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: 2025-11-17



CVE-2025-13299

Descripción: A flaw has been found in itsourcecode Web-Based Internet Laboratory Management System 1.0. This impacts an unknown function of the file /user/controller.php. Executing manipulation can lead to sql injection. The attack may be performed from remote. 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: 2025-11-17



CVE-2025-13300

Descripción: A vulnerability has been found in itsourcecode Web-Based Internet Laboratory Management System 1.0. Affected is an unknown function of the file /settings/controller.php. The manipulation 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: 2025-11-17



CVE-2025-13301

Descripción: A vulnerability was found in itsourcecode Web-Based Internet Laboratory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /subject/controller.php. The manipulation results in sql injection. It is possible to launch the attack 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: 2025-11-17



CVE-2025-13302

Descripción: A vulnerability was identified in code-projects Courier Management System 1.0. This affects an unknown part of the file /add-new-officer.php. Such manipulation of the argument ManagerName leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.

CVSS: 4.7 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-17



CVE-2025-13303

Descripción: A vulnerability was determined in code-projects Courier Management System 1.0. Affected by this issue is some unknown functionality of the file /search-edit.php. This manipulation of the argument Consignment causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-17



CVE-2025-13323

Descripción: A security flaw has been discovered in code-projects Simple Pizza Ordering System 1.0. Affected is an unknown function of the file /listorder.php. Performing 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 exploited.

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: 2025-11-18



CVE-2025-40547

Descripción: A logic error vulnerability exists in Serv-U which when abused could give a malicious actor with access to admin privileges the ability to execute code.

This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.

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-116

Tecnología: No especificado

Publicado el: 2025-11-18



CVE-2025-40548

Descripción: A missing validation process exists in Serv U when abused, could give a malicious actor with access to admin privileges the ability to execute code.

This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.

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-269

Tecnología: No especificado

Publicado el: 2025-11-18



CVE-2025-40549

Descripción: A Path Restriction Bypass vulnerability exists in Serv-U that when abused, could give a malicious actor with access to admin privileges the ability to execute code on a directory.

This issue requires administrative privileges to abuse. On Windows systems, this scored as medium due to differences in how paths and home directories are handled.

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-22

Tecnología: No especificado

Publicado el: 2025-11-18



CVE-2025-41346

Descripción: Faulty authorization control in software WinPlus v24.11.27 by Informática del Este that allows another user to be impersonated simply by knowing their 'numerical ID', meaning that an attacker could compromise another user's account, thereby affecting the confidentiality, integrity, and availability of the data stored in the application.

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: 2025-11-18



CVE-2025-41347

Descripción: Unlimited upload vulnerability for dangerous file types in WinPlus v24.11.27 from Informática del Este. This vulnerability allows an attacker to upload a 'webshell' by sending a POST request to '/WinplusPortal/ws/swinplus.svc/json/uploadfile'.

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: 2025-11-18



CVE-2025-41733

Descripción: The commissioning wizard on the affected devices does not validate if the device is already initialized. An unauthenticated remote attacker can construct POST requests to set root credentials.

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-305

Tecnología: No especificado

Publicado el: 2025-11-18



CVE-2025-41734

Descripción: An unauthenticated remote attacker can execute arbitrary php files and gain full access of the affected devices.

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-98

Tecnología: No especificado

Publicado el: 2025-11-18



CVE-2025-13344

Descripción: A weakness has been identified in SourceCodester Train Station Ticketing System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=login. This manipulation of the argument Username causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.

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: 2025-11-18



CVE-2025-41348

Descripción: SQL injection vulnerability in WinPlus v24.11.27 by Informática del Este. This vulnerability allows an attacker recover, create, update an delete databases by sending a POST request using the parameters 'val1' and 'cont' in '/WinplusPortal/ws/swinplus.svc/json/getacumper_post'.

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: 2025-11-18



CVE-2025-13396

Descripción: A weakness has been identified in code-projects Courier Management System 1.0. This affects an unknown function of the file /add-office.php. This manipulation of the argument OfficeName causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-19



CVE-2025-13400

Descripción: A vulnerability was detected in Tenda CH22 1.0.0.1. Affected is the function formWrlExtraGet of the file /goform/WrlExtraGet. Performing manipulation of the argument chkHz results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-11-19



CVE-2025-13421

Descripción: A security vulnerability has been detected in itsourcecode Human Resource Management System 1.0. Impacted is an unknown function of the file /src/store/NoticeStore.php. Such manipulation of the argument noticeDesc leads to sql injection. The attack can be launched 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: 2025-11-19



CVE-2025-13424

Descripción: A vulnerability has been found in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /admin/add_product.php. The manipulation of the argument txtProductName leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.

CVSS: 4.7 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-11-20



CVE-2025-13445

Descripción: A flaw has been found in Tenda AC21 16.03.08.16. This affects an unknown part of the file /goform/SetIpMacBind. Executing manipulation of the argument list can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-11-20



CVE-2025-13446

Descripción: A vulnerability has been found in Tenda AC21 16.03.08.16. This vulnerability affects unknown code of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone/time leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.

CVSS: 8.8 (HIGH)

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

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-11-20



CVE-2025-13449

Descripción: A vulnerability was found in code-projects Online Shop Project 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument Password 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: 2025-11-20



CVE-2025-13451

Descripción: A vulnerability was identified in SourceCodester Online Shop Project 1.0. The affected element is an unknown function of the file /action.php. Such manipulation of the argument Search 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: 2025-11-20



CVE-2025-59245

Descripción: Microsoft SharePoint Online Elevation of Privilege Vulnerability

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: 2025-11-20



CVE-2025-11456

Descripción: The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the `eh_crm_new_ticket_post()` function in all versions up to, and including, 3.3.1. 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: 2025-11-21



Resumen del Reporte

CVEs analizados: 49

Promedio CVSS: 7.65

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ☺

