CVEs más relevantes de la semana

Del 11/11/2025 al 18/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-60724

Descripción: Heap-based buffer overflow in Microsoft Graphics Component allows an unauthorized attacker to execute code 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-122

Tecnología: No especificado

Publicado el: 2025-11-11

CVE-2025-11366

Descripción: N-central < 2025.4 is vulnerable to authentication bypass via path traversal

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: 2025-11-12

CVE-2025-11367

Descripción: The N-central Software Probe < 2025.4 is vulnerable to Remote Code Execution via deserialization

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: 2025-11-12

CVE-2025-13057

Descripción: A vulnerability was identified in Campcodes School Fees Payment Management System 1.0. Impacted is an unknown function of the file /ajax.php?action=save_student. The manipulation of the argument ID leads to sql injection. The attack may 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: 2025-11-12

CVE-2025-13059

Descripción: A weakness has been identified in SourceCodester Alumni Management System 1.0. The impacted element is an unknown function of the file /manage_career.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. 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: 2025-11-12

CVE-2025-13060

Descripción: A security vulnerability has been detected in SourceCodester Survey Application System 1.0. This affects an unknown function of the file /view_survey.php. Such manipulation of the argument ID 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: 2025-11-12

CVE-2025-13075

Descripción: A vulnerability was detected in code-projects Responsive Hotel Site 1.0. Impacted is an unknown function of the file /admin/usersettingdel.php. Performing manipulation of the argument eid results in sql injection. Remote exploitation of the attack is possible. The exploit is now 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: 2025-11-12

CVE-2025-13076

Descripción: A flaw has been found in code-projects Responsive Hotel Site 1.0. The affected element is an unknown function of the file /admin/usersetting.php. Executing manipulation of the argument usname can lead to sql injection. The attack can be executed remotely. The exploit has been published 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: 2025-11-12

CVE-2025-13122

Descripción: A vulnerability was detected in SourceCodester Patients Waiting Area Queue Management System 1.0. The affected element is the function getPatientAppointment of the file /php/api_patient_checkin.php. Performing manipulation of the argument appointmentID 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: 2025-11-13

CVE-2025-36096

Descripción: IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 stores NIM private keys used in NIM environments in an insecure way which is susceptible to unauthorized access by an attacker using man in the middle techniques.

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-522

Tecnología: No especificado

Publicado el: 2025-11-13

CVE-2025-36250

Descripción: IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 NIM server (formerly known as NIM master) service (nimesis) could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerability that was previously addressed in CVE-2024-56346.

CVSS: 10.0 (CRITICAL)

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

Tipo: CWE-114

Tecnología: No especificado

Publicado el: 2025-11-13

CVE-2025-36251

Descripción: IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 nimsh service SSL/TLS implementations could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerability that was previously addressed in CVE-2024-56347.

CVSS: 9.6 (CRITICAL)

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

Tipo: CWE-114

Tecnología: No especificado

Publicado el: 2025-11-13

CVE-2025-13169

Descripción: A security vulnerability has been detected in code-projects Simple Online Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /add_query_reserve.php. Such manipulation of the argument room_id 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: 2025-11-14

CVE-2025-13170

Descripción: A vulnerability was detected in code-projects Simple Online Hotel Reservation System 1.0. This issue affects some unknown processing of the file /admin/edit_account.php. Performing manipulation of the argument admin_id 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: 2025-11-14

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-2025-40547

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-2025-41733

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

Resumen del Reporte

CVEs analizados: 20

Promedio CVSS: 8.29

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □