CVEs más relevantes de la semana

Del 23/08/2025 al 30/08/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-9397

Descripción: A weakness has been identified in givanz Vvveb up to 1.0.7.2. Affected is an unknown function of the file /system/traits/media.php. Executing manipulation of the argument files[] can lead to unrestricted upload. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. Applying a patch is advised to resolve this issue. The code maintainer exp...

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-284

Tecnología: No especificado

Publicado el: 2025-08-24

CVE-2025-46411

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.

CVSS: 8.1 (HIGH)

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

Tipo: CWE-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-48005

Descripción: A heap-based buffer overflow vulnerability exists in the RHS2000 parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted RHS2000 file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this 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-122

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-52461

Descripción: An out-of-bounds read vulnerability exists in the Nex parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted .nex file can lead to an information leak. An attacker can provide a malicious file to trigger this vulnerability.

CVSS: 8.2 (HIGH)

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

Tipo: CWE-125

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-52581

Descripción: An integer overflow vulnerability exists in the GDF parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted GDF file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this 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-190

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-53511

Descripción: A heap-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this 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-122

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-53518

Descripción: An integer overflow vulnerability exists in the ABF parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted ABF file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this 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-190

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-53557

Descripción: A heap-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this 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-122

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-53853

Descripción: A heap-based buffer overflow vulnerability exists in the ISHNE parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted ISHNE ECG annotations file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this 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-122

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54462

Descripción: A heap-based buffer overflow vulnerability exists in the Nex parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted .nex file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this 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-122

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54480

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8719 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54481

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8744 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54482

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8751 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54483

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8759 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54484

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8779 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54485

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8785 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54486

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8824 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54487

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8842 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54488

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8850 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54489

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8970 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54490

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9090 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54491

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9191 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54492

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9141 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54493

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9184 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-54494

Descripción: A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9205 of biosig.c on the current master branch (35a819fa), when the T...

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-121

Tecnología: No especificado

Publicado el: 2025-08-25

CVE-2025-41702

Descripción: The JWT secret key is embedded in the egOS WebGUI backend and is readable to the default user. An unauthenticated remote attacker can generate valid HS256 tokens and bypass authentication/authorization due to the use of hard-coded cryptographic key.

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-321

Tecnología: No especificado

Publicado el: 2025-08-26

CVE-2025-7775

Descripción: Memory overflow vulnerability leading to Remote Code Execution and/or Denial of Service in NetScaler ADC and NetScaler Gateway when NetScaler is configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server

(OR)

NetScaler ADC and NetScaler Gateway 13.1, 14.1, 13.1-FIPS and NDcPP: LB virtual servers of type (HTTP, SSL or HTTP_QUIC) bound with IPv6 services or ser...

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-119

Tecnología: No especificado

Publicado el: 2025-08-26

CVE-2025-9523

Descripción: A vulnerability was detected in Tenda AC1206 15.03.06.23. Affected is the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.

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-119

Tecnología: No especificado

Publicado el: 2025-08-27

CVE-2025-7955

Descripción: The RingCentral Communications plugin for WordPress is vulnerable to Authentication Bypass due to improper validation within the ringcentral_admin_login_2fa_verify() function in versions 1.5 to 1.6.8. This makes it possible for unauthenticated attackers to log in as any user simply by supplying identical bogus codes.

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-287

Tecnología: No especificado

Publicado el: 2025-08-28

CVE-2025-8857

Descripción: Clinic Image System developed by Changing contains hard-coded Credentials, allowing unauthenticated remote attackers to log into the system using administrator credentials embedded in the source code.

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-798

Tecnología: No especificado

Publicado el: 2025-08-29

CVE-2025-8861

Descripción: TSA developed by Changing has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents.

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: 2025-08-29

Resumen del Reporte

CVEs analizados: 31

Promedio CVSS: 9.58

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat