

RESUMEN DE AVISOS DE SEGURIDAD

Resumen N°09 - 2025

Periodo: 01/08/2025 al 15/08/2025

1. Actualización de seguridad para productos DellPowerProtect

Vulnerabilidades destacadas y criticidad:

- CVE-2025-31651: **CVSS de 9.8**
- CVE-2024-52533: **CVSS de 9.8**
- CVE-2024-45490: **CVSS de 9.8**

Más información:

<https://www.cert.gov.py/actualizacion-de-seguridad-para-productos-dellpowerprotect/>

2. Vulnerabilidad en múltiples productos Apple

Vulnerabilidades destacadas y criticidad:

- CVE-2025-24243: **CVSS de 7.8**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-multiples-productos-apple/>

3. Vulnerabilidades en Microsoft Edge

Vulnerabilidades destacadas y criticidad:

- CVE-2025-8576: **CVSS de 8.8**
- CVE-2025-8578: **CVSS de 8.8**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-microsoft-edge-2/>



4. Múltiples vulnerabilidades en productos Schneider Electric

Vulnerabilidades destacadas y criticidad:

- CVE-2025-54923: **CVSS de 8.8**
- CVE-2025-54924: **CVSS de 8.7**
- CVE-2025-54925: **CVSS de 8.7**

Más información: <https://www.cert.gov.py/multiples-vulnerabilidades-en-productos-schneider-electric/>



5. Múltiples vulnerabilidades en Dell ControlVault3

Vulnerabilidades destacadas y criticidad:

- CVE-2025-25215: **CVSS de 8.8**
- CVE-2025-24922: **CVSS de 8.8**
- CVE-2025-25050: **CVSS de 8.8**

Más información: <https://www.cert.gov.py/multiples-vulnerabilidades-en-dell-controlvault3/>



6. Actualización de seguridad de SAP

Vulnerabilidades destacadas y criticidad:

- CVE-2025-42957: **CVSS de 9.9**
- CVE-2025-42950: **CVSS de 9.9**
- CVE-2025-42951: **CVSS de 8.8**

Más información:

<https://www.cert.gov.py/actualizacion-de-seguridad-de-sap-2/>

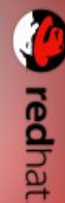


7. Múltiples vulnerabilidades en RedHat Linux

Vulnerabilidades destacadas y criticidad:

- CVE-2025-49796: **CVSS de 9.1**
- CVE-2025-49794: **CVSS de 9.1**
- CVE-2025-22871: **CVSS de 9.1**

Más información: <https://www.cert.gov.py/multiples-vulnerabilidades-en-redhat-linux/>



8. Vulnerabilidad en el kernel de Linux

Vulnerabilidades destacadas y criticidad:

- CVE-2025-38236: **CVSS de 7.8**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-el-kernel-de-linux-2/>



9. Vulnerabilidad en Dell SupportAssist OS Recovery

Vulnerabilidades destacadas y criticidad:

- CVE-2025-38747: CVSS de 7.8

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-dell-supportassist-os-recovery/>

DELL

10. Vulnerabilidad en WinRAR

Vulnerabilidades destacadas y criticidad:

- CVE-2025-8088: CVSS de 8.4

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-winrar/>

WinRAR

11. Vulnerabilidad en productos D-Link

Vulnerabilidades destacadas y criticidad:

- CVE-2020-25079: **CVSS de 8.8**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-productos-d-link/>

D-Link®

12. Actualización de seguridad para Dell Networking OS10

Vulnerabilidades destacadas y criticidad:

- CVE-2024-38428: **CVSS de 9.1**
- CVE-2023-4738: **CVSS de 7.8**
- CVE-2025-4802: **CVSS de 7.8**

Más información:

<https://www.cert.gov.py/actualizacion-de-seguridad-para-dell-networking-os10/>



13. Vulnerabilidades en Adobe Experience Manager Forms

Vulnerabilidades destacadas y criticidad:

- CVE-2025-54253: **CVSS de 10.0**
- CVE-2025-54254: **CVSS de 8.6**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-adobe-experience-manager-forms/>



14. Actualizaciones de seguridad de Android

Vulnerabilidades destacadas y criticidad:

- CVE-2025-48530: **Severidad Crítica**
- CVE-2025-22441: **Severidad Alta**
- CVE-2025-48533: **Severidad Alta**

Más información:

<https://www.cert.gov.py/actualizaciones-de-seguridad-de-android-4/>



15. Vulnerabilidad en node-SAML de JavaScript

Vulnerabilidades destacadas y criticidad:

- CVE-2025-54419: **CVSS de 10.0**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-libreria-node-saml/>



16. Vulnerabilidad en IBM Db2

Vulnerabilidades destacadas y criticidad:

- CVE-2025-33092: **CVSS de 7.8**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-ibm-db2/>



17. Vulnerabilidad en Microsoft Exchange Server

Vulnerabilidades destacadas y criticidad:

- CVE-2025-53786: **CVSS de 8.0**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-microsoft-exchange-server/>



18. Múltiples vulnerabilidades en productos Autodesk

Vulnerabilidades destacadas y criticidad:

- CVE-2025-5038: **CVSS de 7.8**
- CVE-2025-5043: **CVSS de 7.8**
- CVE-2025-6631: **CVSS de 7.8**

Más información: <https://www.cert.gov.py/multiples-vulnerabilidades-en-productos-autodesk-2/>



19. Vulnerabilidad en Tenable Patch Management

Vulnerabilidades destacadas y criticidad:

- CVE-2025-8096: **CVSS de 8.6**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-tenable-patch-management/>



20. Vulnerabilidades en Apache Jena

Vulnerabilidades destacadas y criticidad:

- CVE-2025-50151: **CVSS de 8.8**
- CVE-2025-49656: **CVSS de 7.5**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-apache-jena/>



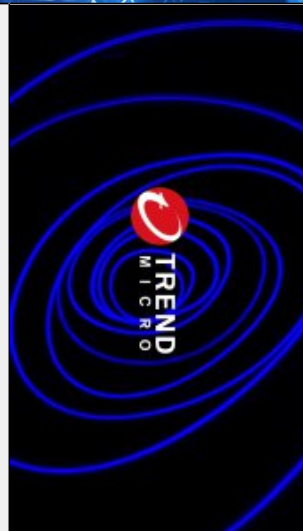
21. Vulnerabilidades en los productos de Trend Micro

Vulnerabilidades destacadas y criticidad:

- CVE-2025-54948: **CVSS de 9.4**
- CVE-2025-54987: **CVSS de 9.4**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-los-productos-de-trend-micro/>



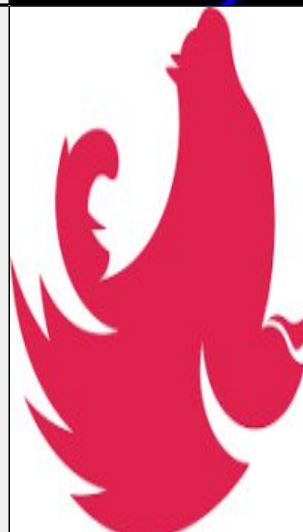
22. Vulnerabilidad en el Framework NestJS

Vulnerabilidades destacadas y criticidad:

- CVE-2025-54782: **CVSS de 9.4**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-el-framework-nestjs/>



23. Vulnerabilidad en el complemento Post SMTP de WordPress

Vulnerabilidades destacadas y criticidad:

- CVE-2025-24000: **CVSS** de 8.8

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-el-complemento-post-smtp-de-wordpress/>



24. Vulnerabilidad en AWS Client VPN de Windows

Vulnerabilidades destacadas y criticidad:

- CVE-2025-8069: **CVSS** de 7.8

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-aws-client-vpn-de-windows/>



25. Vulnerabilidad en SUSE Manager

Vulnerabilidades destacadas y criticidad:

- CVE-2025-46811: **CVSS de 9.8**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-suse-manager/>



26. Vulnerabilidades en firmware UEFI

Vulnerabilidades destacadas y criticidad:

- CVE-2025-4421: **CVSS de 8.2**
- CVE-2025-4422: **CVSS de 8.2**
- CVE-2025-4423: **CVSS de 8.2**
- CVE-2025-4425: **CVSS de 8.2**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-firmware-uefi/>



27. Vulnerabilidades en productos TP-Link

Vulnerabilidades destacadas y criticidad:

- CVE-2025-7724: **CVSS de 8.7**
- CVE-2025-7723: **CVSS de 8.5**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-tp-link/>



28. Vulnerabilidad en productos SonicWall

Vulnerabilidades destacadas y criticidad:

- CVE-2025-40600: **CVSS de 9.8**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-productos-sonicwall-2/>



29. Vulnerabilidades en productos Elastic

Vulnerabilidades destacadas y criticidad:

- CVE-2025-0712: **CVSS de 7.0**
- CVE-2025-25011: **CVSS de 7.0**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-elastic/>



30. Vulnerabilidad en Alone de WordPress

Vulnerabilidades destacadas y criticidad:

- CVE-2025-5394: **CVSS de 9.8**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-alone-de-wordpress/>

