

RESUMEN DE AVISOS DE SEGURIDAD

Resumen N°30 - 2026

Periodo: 01/07/2026 al 15/07/2026

1. Vulnerabilidades en productos WatchGuard

Vulnerabilidades destacadas y criticidad:

- CVE-2026-13368: **CVSS de 9.2**
- CVE-2026-13084: **CVSS de 8.7**
- CVE-2026-13050: **CVSS de 8.6**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-watchguard-5/>



2. Vulnerabilidad en productos MediaTek

Vulnerabilidad destacada y criticidad:

- CVE-2026-20458: **CVSS de 7.5**

Más información:

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



3. Vulnerabilidades en productos GitLab

Vulnerabilidades destacadas y criticidad:

- CVE-2026-6896: **CVSS de 8.7**
- CVE-2026-13320: **CVSS de 7.3**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-15/>



4. Vulnerabilidad en productos Palo Alto

Vulnerabilidad destacada y criticidad:

- CVE-2026-0288: **CVSS de 7.2**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-productos-palo-alto-4/>



5. Vulnerabilidad en productos ASUS

Vulnerabilidad destacada y criticidad:

- CVE-2026-8921: **CVSS de 8.5**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-productos-asus-3/>



6. Vulnerabilidades en productos SSH

Vulnerabilidades destacadas y criticidad:

- CVE-2026-55200: **CVSS de 9.2**
- CVE-2025-15661: **CVSS de 8.3**
- CVE-2026-55199: **CVSS de 8.2**

Más información:

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



7. Vulnerabilidades en productos Elastic

Vulnerabilidades destacadas y criticidad:

- CVE-2026-49091: **CVSS de 8.0**
- CVE-2026-32283: **CVSS de 7.5**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-elastic-4/>



8. Vulnerabilidades en productos Adobe

Vulnerabilidades destacadas y criticidad:

- CVE-2026-48282: **CVSS de 10.0**
- CVE-2026-48276: **CVSS de 10.0**
- CVE-2026-48277: **CVSS de 10.0**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-adobe-6/>



9. Vulnerabilidad en productos Progress

Vulnerabilidad destacada y criticidad:

- CVE-2026-8037: **CVSS de 9.6**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-productos-progress-3/>



10. Vulnerabilidades en productos Cisco

Vulnerabilidades destacadas y criticidad:

- CVE-2026-20217: **CVSS de 7.5**
- CVE-2026-20191: **CVSS de 7.5**
- CVE-2026-20214: **CVSS de 7.5**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-cisco-16/>



11. Vulnerabilidad en productos Apache

Vulnerabilidad destacada y criticidad:

- CVE-2026-55957: **CVSS de 7.3**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-productos-apache-12/>



12. Vulnerabilidades en productos Citrix

Vulnerabilidades destacadas y criticidad:

- CVE-2026-8655: **CVSS de 8.8**
- CVE-2026-8452: **CVSS de 8.8**
- CVE-2026-8451: **CVSS de 8.8**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-citrix-4/>

CITRIX

13. Vulnerabilidades en productos Ubiquiti

Vulnerabilidades destacadas y criticidad:

- CVE-2026-34910: **CVSS de 10.0**
- CVE-2026-34908: **CVSS de 10.0**
- CVE-2026-34909: **CVSS de 10.0**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-ubiquiti-4/>

UBIQUITI
NETWORKS

14. Vulnerabilidades en productos JetBrains

Vulnerabilidades destacadas y criticidad:

- CVE-2026-50242: **CVSS de 10.0**
- CVE-2026-56141: **CVSS de 9.8**
- CVE-2026-56142: **CVSS de 9.6**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-jetbrains-2/>

JETBRAINS

15. Vulnerabilidad en productos Zoho

Vulnerabilidad destacada y criticidad:

- CVE-2026-11374: **CVSS de 9.0**

Más información:

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



16. Vulnerabilidad en productos TP-Link

Vulnerabilidad destacada y criticidad:

- CVE-2026-11834: **CVSS de 8.7**

Más información:

<https://www.cert.gov.py/vulnerabilidad-en-productos-tp-link-5/>



17. Vulnerabilidades en productos Cacti

Vulnerabilidades destacadas y criticidad:

- CVE-2026-39938: **CVSS de 9.8**
- CVE-2026-39955: **CVSS de 9.8**
- CVE-2026-39893: **CVSS de 9.8**

Más información:

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



18. Vulnerabilidades en productos GitLab

Vulnerabilidades destacadas y criticidad:

- CVE-2026-10086: **CVSS de 8.7**
- CVE-2026-12053: **CVSS de 8.6**
- CVE-2026-10712: **CVSS de 8.0**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-14/>



19. Vulnerabilidades en productos MISP

Vulnerabilidades destacadas y criticidad:

- CVE-2026-56422: **CVSS de 9.4**
- CVE-2026-56423: **CVSS de 9.4**
- CVE-2026-56447: **CVSS de 9.3**

Más información:

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



20. Vulnerabilidades en productos Grafana

Vulnerabilidades destacadas y criticidad:

- CVE-2026-28381: **CVSS de 9.6**
- CVE-2026-42129: **CVSS de 7.7**
- CVE-2026-42127: **CVSS de 7.5**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-grafana-3/>



21. Vulnerabilidad en producto Autodesk

Vulnerabilidad destacada y criticidad:

- CVE-2026-10789: **CVSS de 9.6**

Más información:

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



22. Vulnerabilidades en productos Spring

Vulnerabilidades destacadas y criticidad:

- CVE-2026-41862: **CVSS de 8.8**
- CVE-2026-40999: **CVSS de 8.6**
- CVE-2026-47825: **CVSS de 8.6**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-spring-10/>



23. Vulnerabilidades en productos Splunk

Vulnerabilidades destacadas y criticidad:

- CVE-2026-20253: **CVSS de 9.8**
- CVE-2026-20251: **CVSS de 8.8**
- CVE-2026-20252: **CVSS de 7.6**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-splunk-6/>



24. Vulnerabilidades en productos Atlassian

Vulnerabilidades destacadas y criticidad:

- CVE-2026-41293: **CVSS de 9.8**
- CVE-2026-43512: **CVSS de 9.8**
- CVE-2026-43515: **CVSS de 9.1**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-atlassian-4/>

ATLASSIAN

25. Vulnerabilidad en productos Avast

Vulnerabilidad destacada y criticidad:

- CVE-2025-71326: **CVSS de 8.5**

Más información:

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



26. Vulnerabilidades en productos Nginx

Vulnerabilidades destacadas y criticidad:

- CVE-2026-42055: **CVSS de 9.2**
- CVE-2026-42530: **CVSS de 9.2**
- CVE-2026-11311: **CVSS de 8.6**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-nginx-2/>



27. Vulnerabilidades en productos Node.js

Vulnerabilidades destacadas y criticidad:

- CVE-2026-48618: **CVSS de 7.7**
- CVE-2026-48933: **CVSS de 7.5**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-node-js-2/>



28. Vulnerabilidad en productos Drupal

Vulnerabilidad destacada y criticidad:

- CVE-2026-55803: **CVSS de 8.8**

Más información:

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



29. Vulnerabilidades en productos QNAP

Vulnerabilidades destacadas y criticidad:

- CVE-2026-44083: **CVSS de 8.7**
- CVE-2026-26236: **CVSS de 7.5**
- CVE-2026-26237: **CVSS de 7.5**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-qnap-5/>



30. Vulnerabilidades en productos Ubiquiti

Vulnerabilidades destacadas y criticidad:

- CVE-2026-47370: **CVSS de 9.9**
- CVE-2026-47369: **CVSS de 9.9**
- CVE-2026-47367: **CVSS de 9.9**

Más información:

<https://www.cert.gov.py/vulnerabilidades-en-productos-ubiquiti-3/>

