



**CERT-PY**

# RESUMEN DE CVEs DESTACADOS

Resumen N°14 - 2026

Periodo: 01/05/2026 al 31/05/2026

| CVE            | Proveedor | Más información   |
|----------------|-----------|---|
| CVE-2026-29205 | cPanel    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel-2/</a>   |
| CVE-2026-32992 | cPanel    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel-2/</a>   |
| CVE-2026-32993 | cPanel    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel-2/</a>   |
| CVE-2026-9136  | Misp      | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-misp/">https://www.cert.gov.py/vulnerabilidad-en-productos-misp/</a>               |
| CVE-2026-41091 | Microsoft | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-microsoft-9/">https://www.cert.gov.py/vulnerabilidad-en-productos-microsoft-9/</a> |
| CVE-2026-23898 | Joomla    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-joomla/">https://www.cert.gov.py/vulnerabilidades-en-productos-joomla/</a>       |
| CVE-2026-23899 | Joomla    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-joomla/">https://www.cert.gov.py/vulnerabilidades-en-productos-joomla/</a>       |
| CVE-2026-2740  | Zoho      | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-zoho/">https://www.cert.gov.py/vulnerabilidad-en-productos-zoho/</a>               |
| CVE-2026-48829 | GNU       | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-gnu-3/">https://www.cert.gov.py/vulnerabilidad-en-productos-gnu-3/</a>             |
| CVE-2026-41705 | Spring    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-spring-8/">https://www.cert.gov.py/vulnerabilidades-en-productos-spring-8/</a>   |
| CVE-2026-41712 | Spring    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-spring-8/">https://www.cert.gov.py/vulnerabilidades-en-productos-spring-8/</a>   |
| CVE-2026-41713 | Spring    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-spring-8/">https://www.cert.gov.py/vulnerabilidades-en-productos-spring-8/</a>   |
| CVE-2026-6073  | GitLab    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-11/">https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-11/</a> |
| CVE-2026-7377  | GitLab    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-11/">https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-11/</a> |
| CVE-2026-7481  | GitLab    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-11/">https://www.cert.gov.py/vulnerabilidades-en-productos-gitlab-11/</a> |
| CVE-2026-45281 | Nextcloud | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-nextcloud-2/">https://www.cert.gov.py/vulnerabilidad-en-productos-nextcloud-2/</a> |
| CVE-2026-8843  | MongoDB   | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-mongodb-3/">https://www.cert.gov.py/vulnerabilidad-en-productos-mongodb-3/</a>     |
| CVE-2026-33377 | Grafana   | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-grafana-4/">https://www.cert.gov.py/vulnerabilidad-en-productos-grafana-4/</a>     |
| CVE-2026-20224 | Cisco     | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-cisco-6/">https://www.cert.gov.py/vulnerabilidad-en-productos-cisco-6/</a>         |
| CVE-2026-7256  | Zyxel     | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-zyxel/">https://www.cert.gov.py/vulnerabilidad-en-productos-zyxel/</a>             |
| CVE-2026-41702 | VMware    | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-vmware-3/">https://www.cert.gov.py/vulnerabilidad-en-productos-vmware-3/</a>       |
| CVE-2026-8260  | D-Link    | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-d-link-3/">https://www.cert.gov.py/vulnerabilidad-en-productos-d-link-3/</a>       |

| CVE            | Proveedor  | Más información   |
|----------------|------------|---|
| CVE-2026-6473  | PostgreSQL | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-postgresql-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-postgresql-2/</a> |
| CVE-2026-6475  | PostgreSQL | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-postgresql-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-postgresql-2/</a> |
| CVE-2026-6477  | PostgreSQL | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-postgresql-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-postgresql-2/</a> |
| CVE-2026-0264  | Palo Alto  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-palo-alto-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-palo-alto-2/</a>   |
| CVE-2026-0265  | Palo Alto  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-palo-alto-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-palo-alto-2/</a>   |
| CVE-2025-0327  | Schneider  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-schneider-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-schneider-2/</a>   |
| CVE-2026-4827  | Schneider  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-schneider-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-schneider-2/</a>   |
| CVE-2026-6866  | Schneider  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-schneider-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-schneider-2/</a>   |
| CVE-2026-41288 | WatchGuard | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-watchguard-4/">https://www.cert.gov.py/vulnerabilidades-en-productos-watchguard-4/</a> |
| CVE-2026-6787  | WatchGuard | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-watchguard-4/">https://www.cert.gov.py/vulnerabilidades-en-productos-watchguard-4/</a> |
| CVE-2026-6788  | WatchGuard | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-watchguard-4/">https://www.cert.gov.py/vulnerabilidades-en-productos-watchguard-4/</a> |
| CVE-2026-23479 | Redis      | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-redis/">https://www.cert.gov.py/vulnerabilidades-en-productos-redis/</a>               |
| CVE-2026-25588 | Redis      | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-redis/">https://www.cert.gov.py/vulnerabilidades-en-productos-redis/</a>               |
| CVE-2026-25589 | Redis      | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-redis/">https://www.cert.gov.py/vulnerabilidades-en-productos-redis/</a>               |
| CVE-2026-3828  | Hikvision  | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-hikvision-3/">https://www.cert.gov.py/vulnerabilidad-en-productos-hikvision-3/</a>       |
| CVE-2025-40949 | Siemens    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-siemens-6/">https://www.cert.gov.py/vulnerabilidades-en-productos-siemens-6/</a>       |
| CVE-2026-25786 | Siemens    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-siemens-6/">https://www.cert.gov.py/vulnerabilidades-en-productos-siemens-6/</a>       |
| CVE-2026-25787 | Siemens    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-siemens-6/">https://www.cert.gov.py/vulnerabilidades-en-productos-siemens-6/</a>       |
| CVE-2026-6022  | Progress   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-progress-4/">https://www.cert.gov.py/vulnerabilidades-en-productos-progress-4/</a>     |
| CVE-2026-6023  | Progress   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-progress-4/">https://www.cert.gov.py/vulnerabilidades-en-productos-progress-4/</a>     |
| CVE-2026-41615 | Microsoft  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-microsoft-9/">https://www.cert.gov.py/vulnerabilidades-en-productos-microsoft-9/</a>   |
| CVE-2026-42897 | Microsoft  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-microsoft-9/">https://www.cert.gov.py/vulnerabilidades-en-productos-microsoft-9/</a>   |

| CVE            | Proveedor | Más información   |
|----------------|-----------|---|
| CVE-2026-6722  | php       | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-php/">https://www.cert.gov.py/vulnerabilidad-en-productos-php/</a>                   |
| CVE-2026-40981 | Spring    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-spring-7/">https://www.cert.gov.py/vulnerabilidades-en-productos-spring-7/</a>     |
| CVE-2026-40982 | Spring    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-spring-7/">https://www.cert.gov.py/vulnerabilidades-en-productos-spring-7/</a>     |
| CVE-2026-41002 | Spring    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-spring-7/">https://www.cert.gov.py/vulnerabilidades-en-productos-spring-7/</a>     |
| CVE-2026-20034 | Cisco     | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cisco-15/">https://www.cert.gov.py/vulnerabilidades-en-productos-cisco-15/</a>     |
| CVE-2026-20167 | Cisco     | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cisco-15/">https://www.cert.gov.py/vulnerabilidades-en-productos-cisco-15/</a>     |
| CVE-2026-20185 | Cisco     | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cisco-15/">https://www.cert.gov.py/vulnerabilidades-en-productos-cisco-15/</a>     |
| CVE-2026-6691  | MongoDB   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-mongodb-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-mongodb-2/</a>   |
| CVE-2026-8063  | MongoDB   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-mongodb-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-mongodb-2/</a>   |
| CVE-2026-41096 | Microsoft | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-microsoft-8/">https://www.cert.gov.py/vulnerabilidad-en-productos-microsoft-8/</a>   |
| CVE-2026-30893 | Wazuh     | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-wazuh-2/">https://www.cert.gov.py/vulnerabilidad-en-productos-wazuh-2/</a>           |
| CVE-2026-44573 | Next.js   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-next-js/">https://www.cert.gov.py/vulnerabilidades-en-productos-next-js/</a>       |
| CVE-2026-44574 | Next.js   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-next-js/">https://www.cert.gov.py/vulnerabilidades-en-productos-next-js/</a>       |
| CVE-2026-44578 | Next.js   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-next-js/">https://www.cert.gov.py/vulnerabilidades-en-productos-next-js/</a>       |
| CVE-2026-29202 | cPanel    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel/">https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel/</a>         |
| CVE-2026-29203 | cPanel    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel/">https://www.cert.gov.py/vulnerabilidades-en-productos-cpanel/</a>         |
| CVE-2026-0300  | Palo Alto | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-palo-alto-2/">https://www.cert.gov.py/vulnerabilidad-en-productos-palo-alto-2/</a>   |
| CVE-2026-23926 | Zabbix    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-zabbix-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-zabbix-2/</a>     |
| CVE-2026-23928 | Zabbix    | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-zabbix-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-zabbix-2/</a>     |
| CVE-2026-25254 | Qualcomm  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-qualcomm-7/">https://www.cert.gov.py/vulnerabilidades-en-productos-qualcomm-7/</a> |
| CVE-2026-25255 | Qualcomm  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-qualcomm-7/">https://www.cert.gov.py/vulnerabilidades-en-productos-qualcomm-7/</a> |
| CVE-2026-25293 | Qualcomm  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-qualcomm-7/">https://www.cert.gov.py/vulnerabilidades-en-productos-qualcomm-7/</a> |

| CVE            | Proveedor | Más información   |
|----------------|-----------|---|
| CVE-2025-11083 | Juniper   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-juniper-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-juniper-2/</a>   |
| CVE-2025-38129 | Juniper   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-juniper-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-juniper-2/</a>   |
| CVE-2025-38248 | Juniper   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-juniper-2/">https://www.cert.gov.py/vulnerabilidades-en-productos-juniper-2/</a>   |
| CVE-2026-0073  | Android   | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-android-2/">https://www.cert.gov.py/vulnerabilidad-en-productos-android-2/</a>       |
| CVE-2026-35228 | Oracle    | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-oracle-6/">https://www.cert.gov.py/vulnerabilidad-en-productos-oracle-6/</a>         |
| CVE-2026-43284 | Linux     | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-linux-2/">https://www.cert.gov.py/vulnerabilidad-en-productos-linux-2/</a>           |
| CVE-2026-4670  | Progress  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-progress-3/">https://www.cert.gov.py/vulnerabilidades-en-productos-progress-3/</a> |
| CVE-2026-5174  | Progress  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-progress-3/">https://www.cert.gov.py/vulnerabilidades-en-productos-progress-3/</a> |
| CVE-2026-6914  | MongoDB   | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-mongodb-2/">https://www.cert.gov.py/vulnerabilidad-en-productos-mongodb-2/</a>       |
| CVE-2026-41882 | JetBrains | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-jetbrains-3/">https://www.cert.gov.py/vulnerabilidad-en-productos-jetbrains-3/</a>   |
| CVE-2026-0204  | Sonicwall | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-sonicwall-3/">https://www.cert.gov.py/vulnerabilidad-en-productos-sonicwall-3/</a>   |
| CVE-2026-41316 | Ruby      | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-ruby/">https://www.cert.gov.py/vulnerabilidad-en-productos-ruby/</a>                 |
| CVE-2026-23918 | Apache    | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-apache-10/">https://www.cert.gov.py/vulnerabilidad-en-productos-apache-10/</a>       |
| CVE-2026-44193 | OPNsense  | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-opnsense/">https://www.cert.gov.py/vulnerabilidad-en-productos-opnsense/</a>         |
| CVE-2026-31931 | Suricata  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-suricata/">https://www.cert.gov.py/vulnerabilidades-en-productos-suricata/</a>     |
| CVE-2026-31934 | Suricata  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-suricata/">https://www.cert.gov.py/vulnerabilidades-en-productos-suricata/</a>     |
| CVE-2026-31935 | Suricata  | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-suricata/">https://www.cert.gov.py/vulnerabilidades-en-productos-suricata/</a>     |
| CVE-2026-7320  | Mozilla   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-mozilla-10/">https://www.cert.gov.py/vulnerabilidades-en-productos-mozilla-10/</a> |
| CVE-2026-7321  | Mozilla   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-mozilla-10/">https://www.cert.gov.py/vulnerabilidades-en-productos-mozilla-10/</a> |
| CVE-2026-7324  | Mozilla   | <a href="https://www.cert.gov.py/vulnerabilidades-en-productos-mozilla-10/">https://www.cert.gov.py/vulnerabilidades-en-productos-mozilla-10/</a> |
| CVE-2026-41940 | cPanel    | <a href="https://www.cert.gov.py/vulnerabilidad-en-productos-cpanel/">https://www.cert.gov.py/vulnerabilidad-en-productos-cpanel/</a>             |