Incident watch

Incident watch — October 2026

Four public information-security incidents in Uruguay in October. The two that took services down, a fiber cut and the PHP2Shell takedown, had no attacker behind them.

4

Incidents logged

Public reports from Uruguay with enough detail to classify.

DATE
October 29, 2026

CODE
WB-IW-2026-10

VERSION
v1.0

EDITION
Public edition

IN BRIEF

1 **October's biggest outages weren't attacks**
Four public incidents in Uruguay.

2 **PHP2Shell: the takedown was the control**
Government sites went dark on purpose, before anyone got in.

3 **The four, and what would have stopped each one**
Cause as reported.

01

October's biggest outages weren't attacks

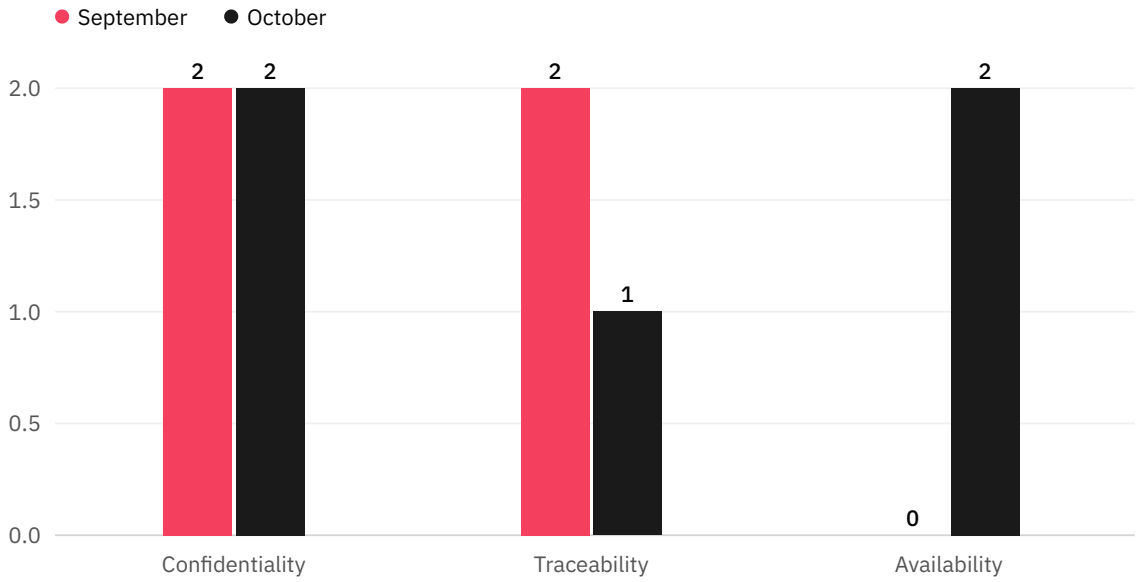
Four public incidents in Uruguay. The two that took services down had no intruder behind them.

Incidents logged
4
Public reports from Uruguay with enough detail to classify.

Outages with no attacker
2
A fiber cut and a preventive takedown.

Procurement systems offline
5
ARCE, since the afternoon of Oct 22. Its Oct 26 notice gives no restore date.

What was hit, September vs. October (one incident can hit two)



Four incidents, five marks on the chart: the fake Sucive raffle hit both confidentiality and traceability.

02

PHP2Shell: the takedown was the control

Government sites went dark on purpose, before anyone got in.

Severity, both flaws
9.2
CVSS v4.0. Unauthenticated remote code execution, per php.net.

Patch and local alert
Oct 21
CERTuy: no known active exploitation at the time.

Listed as exploited
Oct 26
CISA added both to its catalog, per Canada's Cyber Centre.

Oct 20
PHP pre-announces two critical flaws
CVE-2026-109618 and CVE-2026-109619.

Oct 21
Fixes ship, CERTuy alerts
PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35.

Oct 21–22
Ministry portals taken down to patch
Agesic expected them back by Oct 23.

Oct 22
ARCE pulls five systems
Bid openings to be rescheduled.

Oct 26
Active exploitation confirmed
Both flaws in CISA's exploited catalog.

> **What it touches**
> Any PHP server answering web requests, which in CERTuy's list includes WordPress, Drupal, Joomla and Moodle. The gub.uy portals run on Drupal.

03

The four, and what would have stopped each one

Cause as reported. The risk and the control, in plain words.

Incident	What caused it	The risk	What would have stopped it
UTEC, Oct 1. Profile data offered on a dark-web forum.	Automated queries pulling names and photos from its Moodle profiles. UTEC found no database access and no passwords taken.	Someone with access walks the site and pulls everything, page by page.	A per-session read limit that slows down and flags bulk requests. UTEC detected and stopped it itself.
Fake Sucive raffle, Oct 2. US$1,850 moved out of a victim's account.	A sponsored Facebook post led to a fake site that took bank details and the SMS code.	A code that wasn't theirs got used, and an ad passed for the real agency.	A second factor that can't be relayed, like a passkey, instead of a code a person can type into any site.
Antel, Oct 13. Nationwide internet outage.	Four cuts in its fiber transport network, per Antel's report.	Something the service depends on, outside its control, went down.	Degrade, don't fail: what runs on the link keeps working in a reduced mode, like a backup link for payments.
State portals and ARCE, Oct 21–22.	Two critical PHP flaws. Sites taken down to patch. No attacks confirmed in Uruguay.	Something the service depends on, outside its control, went down.	An up-to-date inventory of what runs PHP lets you patch instead of shutting everything down.

04

Sources

1. php.net — critical security releases, Oct 20, 21 and 23, 2026
   www.php.net/
2. CERTuy — Vulnerabilidades críticas en PHP (Oct 21, 2026)
   www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/vulnerabilidades-criticas-php
3. Canadian Centre for Cyber Security — AL26-026 (Oct 21, 2026, updated Oct 27)
   cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619

4. ARCE — Baja de los sistemas (Oct 26, 2026)
www.gub.uy/agencia-reguladora-compras-estatales/comunicacion/noticias/baja-sistemas
5. El Observador — state sites down and servers exposed (Oct 23, 2026)
www.elobservador.com.uy/ciencia-y-tecnologia/sitios-del-estado-caidos-y-miles-servidores-expuestos-el-impacto-uruguay-la-falla-php-n6061404
6. Montevideo Portal — Antel's official report on four fiber cuts (Oct 13, 2026)
www.montevideo.com.uy/Noticias/Cuatro-cortes-de-fibra-optica-el-reporte-oficial-de-Antel-sobre-que-paso-con-internet-uc978461
7. Montevideo Portal — UTEC statement on Moodle (Oct 1, 2026)
www.montevideo.com.uy/Noticias/Alertan-por-filtracion-de-datos-de-UTEC-a-la-dark-web-que-dijo-la-universidad-uc977180
8. Montevideo Portal — fake Sucive raffle, Colonia police report (Oct 2, 2026)
www.montevideo.com.uy/Noticias/Una-mujer-fue-estafada-en-Colonia-se-anoto-en-redes-a-un-falso-sorteo-de-patente-gratis-uc977329

This is the public edition. We produce private editions with your data — for your sector, your operation and the rules that apply to you.

workbigly.com