PAPER TÉCNICO | BOLETÍN EXTRAORDINARIO

Revisión integral de vulnerabilidades, parches y explotación activa

Ventana de vigilancia: 29/10/2026, 08:47 – 30/10/2026, 16:47 (Argentina, UTC−03:00).

Ámbito: organismos públicos, empresas, centros de datos, redes perimetrales, servidores, puestos de trabajo y proveedores tecnológicos.

Clasificación de difusión: TLP:CLEAR | Versión: 1.0 | Fecha de corte: 30 de octubre de 2026.

Documento elaborado para la evaluación preventiva de riesgos y la toma de decisiones de mantenimiento, investigación y continuidad operativa. No constituye por sí mismo una constatación de vulnerabilidad o intrusión en una organización concreta.

Resumen ejecutivo

En las 32 horas examinadas se verificaron hechos nuevos o actualizados relevantes: Google distribuyó Chrome 156.0.8078.79/.80 con 21 correcciones; CISA incorporó el 29/10 dos vulnerabilidades explotadas (GitLab CVE-2026-97229 y Cisco CVE-2026-76418); Palo Alto Networks actualizó el 29/10 su aviso sobre dos fallas PHP de PAN-OS con madurez de explotación “ATTACKED”; el 30/10 se publicó el registro CVE-2026-118539 para Drupal Commerce Core, cuyo aviso del 28/10 ya reconocía explotación activa. [R01–R05]

Se integran, además, asuntos críticos de seguimiento que se originaron antes del intervalo pero cambiaron de relevancia operativa: PolyShell en Adobe Commerce/Magento, actividad maliciosa asociada con VMware ESX, el paquete de endurecimiento de Fortinet, los parches de Oracle/Java y la situación de Microsoft Exchange, Microsoft Authenticator, IBM Db2, Firefox/Thunderbird, Node.js y otras plataformas. Incluirlos no significa afirmar que fueron descubiertos en esta ventana. [R06–R16]

La prioridad técnica no se deriva exclusivamente de CVSS. Se combinan explotación observada, existencia de corrección, exposición a Internet, capacidad para afectar autenticación o virtualización, sensibilidad de información y posibilidades reales de detección. En particular, CVE-2026-41709 de ESX posee CVSS bajo, pero merece tratamiento forense prioritario porque reduce la trazabilidad de acciones administrativas. [R07]

1. Metodología, criterios y límites

Se contrastaron avisos de fabricantes (Google, Mozilla, Cisco, GitLab, Palo Alto Networks, Adobe, Broadcom, Fortinet, Microsoft mediante referencias disponibles, Oracle, IBM, Drupal y Node.js), la lista CISA Known Exploited Vulnerabilities (KEV), autoridades CERT y prensa técnica. El objetivo es discriminar evidencia primaria de información secundaria y evitar confundir CVE asignado con explotación real.

- A — Novedad en ventana: publicación o actualización fechada dentro de las 32 horas.
- B — Evento de explotación/KEV en ventana: fallo anterior que adquirió evidencia nueva y verificable dentro de la ventana.
- C — Antecedente crítico: publicación o actualización anterior; se conserva por su impacto operativo y falta potencial de aplicación del parche.
- D — Verificación pendiente: referencia o hipótesis que no permite atribuir, con suficiente certeza, disponibilidad de parche o explotación activa.

Fecha de publicación, fecha de actualización del boletín, incorporación a KEV y fecha presunta de explotación son conceptos distintos. La disponibilidad de una corrección es un hecho del proveedor; el grado de exposición de cada institución requiere inventario y constatación independiente.

2. Matriz ejecutiva consolidada

Tecnología / CVE	Hecho confirmado y fecha	Estado / Acción
Chrome 156; CVE-2026-76024 y otros	29/10: 21 correcciones (A)	Actualizar a 156.0.8078.79/.80 (Win/Mac) o .79 (Linux).
Cisco ASA/FTD; CVE-2026-76418	29/10: alta en CISA KEV (B)	Explotación confirmada; parchear SSL VPN; sin workaround oficial.
GitLab; CVE-2026-97229	29/10: alta en CISA KEV (B)	RCE sin autenticación; actualizar a rama corregida.
PAN-OS; CVE-2026-109618/109619	29/10: actualización aviso (A)	RCE; “ATTACKED”; parche por subrama y restringir gestión.
Drupal Commerce; CVE-2026-118539	30/10: registro CVE (A); aviso 28/10	Explotación activa; actualizar 2.41 / 3.3.13.
VMware ESX; CVE-2026-41709	28/10: alta KEV (C); cobertura 29/10	Ocultamiento de acciones administrativas; revisar y corregir.
Adobe/Magento; CVE-2026-48356	27/10: KEV (C); alertas 29/10	PolyShell, carga peligrosa; versión -2026-jul.
Fortinet FortiOS y asociados	21–22/10: hardening release (C)	Actualizar ramas afectadas; CVE detallados pendientes.
Microsoft Exchange; CVE-2026-62911	11/08: parche disponible (C)	Revisar SU/ESU y accesos de Exchange local.
Microsoft Authenticator; CVE-2026-80097	08/09: publicación (C/D)	Investigar matriz MSRC; no atribuir RCE ni KEV sin prueba.
Oracle / Java SE / E-Business	20/10: CPU trimestral (C)	1295 parches totales; 55 Java SE; 194 EBS.
IBM Db2 11.5/12.1	08/10: actualizaciones DB2 (C)	Validar Security Update por versión y componentes.
Firefox 159 / Thunderbird	27/10: avisos (C)	Aplicar actualizaciones de Mozilla y ESR.
Node.js 22/24/26	21/10: seguridad; 28/10: releases (C)	Validar ramas LTS, dependencias y despliegue.

3. Novedades confirmadas dentro del intervalo

3.1. Google Chrome — 21 correcciones publicadas el 29 de octubre

El canal Stable y Extended Stable pasó a 156.0.8078.79/.80 en Windows y macOS y 156.0.8078.79 en Linux. La versión introduce 21 correcciones de seguridad; destaca CVE-2026-76024 (corrupción de memoria en MediaStream, severidad crítica), además de fallas de uso después de liberación, corrupción de memoria y validación de entrada en FileSystem, Autofill, CacheStorage, Network, Input, V8, Skia y DOM. El aviso de Google no afirma explotación activa para cada una de las 21 fallas. [R01]

Acción: asegurar despliegue administrado con validación de versión real en estaciones Windows, Linux y macOS. La actualización del 27/10 a Chrome 156.0.8078.73/.74 corregía otras 52 fallas y constituye antecedente inmediato, no una publicación de la ventana. [R01, R15]

3.2. GitLab — CVE-2026-97229 en catálogo CISA KEV

La falla consiste en un desbordamiento de entero en el compilador de expresiones regulares aplicado a configuraciones CI/CD; puede permitir ejecución arbitraria de código desde un usuario no autenticado en

determinadas condiciones. GitLab publicó la corrección crítica el 21/10 en las versiones 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10 y 18.11.13. CISA la incorporó a KEV el 29/10. [R02, R03]

Precisión: GitLab emitió el 29/10 nuevas versiones 19.5.3, 19.4.5, 19.3.7, 19.2.10, 19.1.10, 19.0.11 y 18.11.14, pero el fabricante indicó expresamente que ese lanzamiento NO añade correcciones de seguridad; por lo tanto, no debe registrarse como un nuevo parche del CVE. [R03]

Acción: constatar versión y rama, asegurar actualización acumulativa, revisar jobs, runners, credenciales CI/CD, proyectos sensibles, tokens y modificaciones no autorizadas.

3.3. Cisco ASA/FTD — CVE-2026-76418, SSL VPN

Cisco publicó inicialmente el aviso el 28/10. CISA agregó la vulnerabilidad a KEV el 29/10. CVSS 8.6: un atacante remoto sin autenticación puede provocar la recarga inesperada del firewall y denegación de servicio cuando el servicio de acceso remoto SSL VPN está habilitado y se utiliza autenticación secundaria en el grupo de túnel aplicable. No equivale a ejecución remota de código ni a robo de credenciales demostrado. Cisco señala que no existe workaround que resuelva el problema. [R02, R04]

Acción: identificar ASA/FTD con SSL VPN, inspeccionar configuración webvpn y secondary-authentication-server-group, comparar la versión exacta con la sección Fixed Software de Cisco y programar actualización. Preservar eventos previos a reinicios, tiempos de caída, telemetría de balanceo y registros del concentrador VPN.

3.4. Palo Alto PAN-OS — actualización del 29/10 sobre PHP2Shell

El aviso del 21/10 fue actualizado el 29/10. CVE-2026-109618 y CVE-2026-109619 afectan gestión web de versiones PAN-OS específicas por manejo incorrecto de memoria y estados internos PHP. Palo Alto clasifica el caso como crítico, CVSS 4.0: 9.2, y madurez de explotación “ATTACKED”. La exposición a Internet del plano de administración aumenta de forma sustancial el riesgo. Portal GlobalProtect o Captive Portal no están automáticamente incluidos salvo configuraciones particulares de administración. [R05]

Para ramas 12.2, 12.1, 11.2, 11.1 y 10.2 deben consultarse las distintas subramas hotfix del aviso: p. ej. 12.2.4-h1, 11.2.10-h16 o 10.2.18-h13 para las respectivas líneas. No es correcto sustituir una subrama por otra sin validar el procedimiento oficial. La falla separada CVE-2026-111497 (Brotli) obliga en ciertos casos a versiones más nuevas, por ejemplo 11.2.10-h17; el fabricante no confirma explotación maliciosa de Brotli. [R05, R13]

Acción: cerrar administración pública, exigir acceso mediante bastión y redes de confianza, inventariar perfiles de gestión asociados, instalar corrección adecuada y comparar registros administrativos previos y posteriores. Las firmas de Threat Prevention y la inspección TLS aplican sólo cuando la arquitectura reúne los requisitos de mitigación documentados por Palo Alto. [R05]

3.5. Drupal Commerce Core — CVE-2026-118539

El boletín SA-CONTRIB-2026-254 se publicó el 28/10 y el identificador CVE apareció el 30/10. Drupal clasifica el fallo de autorización como altamente crítico y reconoce explotación activa. Las versiones vulnerables son anteriores a 2.41 en la línea 2.x y desde 3.0.0 hasta antes de 3.3.13 en la 3.x. [R06]

Acción: actualizar a Commerce Core 8.x-2.41 o 3.3.13 según rama; auditar pedidos, precios, estados, autorizaciones y operaciones anómalas. La mera existencia del módulo no prueba compromiso.

4. Riesgos precedentes aún prioritarios

4.1. Adobe Commerce / Magento — PolyShell, CVE-2026-48356

Adobe corrigió en julio la carga sin restricción suficiente de archivos de tipo peligroso. CVSS 9.6, CWE-434; no se requieren credenciales según APSB26-73. La cadena denominada PolyShell permite que un archivo que aparente imagen contenga contenido ejecutable, cuya explotación posterior depende de la configuración web. El hecho de su incorporación a KEV el 27/10 y la difusión de alertas el 29/10 justifican su inclusión como antecedente activo y no como CVE descubierto en las últimas 32 horas. [R08]

Acción: actualizar a los paquetes con sufijo "-2026-jul" o posterior para la rama instalada. Impedir interpretación de PHP en pub/media/custom_options/, limitar subida por API mediante controles aplicables, buscar .php/.phtml/.phar inesperados y revisar contenidos alterados en cms_block y cms_page. Conservar copias, hashes, datos de acceso y evidencias antes de limpiar.

4.2. Broadcom VMware ESX/vCenter — CVE-2026-41709 y VMSA-2026-0006

CVE-2026-41709 (CVSS 2.7) afecta el registro de determinadas operaciones administrativas en ESX. Requiere privilegios elevados; no constituye por sí misma la puerta de entrada. CISA la incorporó a KEV el 28/10. El mismo aviso de Broadcom contiene CVE-2026-59309 (bypass de autenticación en vCenter; 9.8) y CVE-2026-59310 (recorrido de rutas en servidor Syslog vCenter con posible ejecución de código; 9.8). [R07]

Acción: revisar VMSA-2026-0006 y su matriz por producto y compilación; considerar las actualizaciones acumulativas posteriores: por ejemplo ESXi 8 U3k incluye correcciones adicionales. Es esencial extraer y custodiar fuentes de registro externas al hipervisor porque los logs locales pueden ser incompletos, y correlacionar VPN, vCenter, IAM, MFA, EDR, backups y conexiones a la capa de virtualización. La búsqueda de BRICKSTORM debe basarse en indicadores y evidencia, sin presuponer infección.

4.3. Fortinet — paquete coordinado de endurecimiento de octubre

Fortinet comunicó el 21/10 actualizaciones coordinadas disponibles a partir del 22/10 para FortiOS, FortiManager, FortiAnalyzer y, previamente, FortiMail/FortiAuthenticator. Para FortiOS, las compilaciones objetivo anunciadas son 8.0.2, 7.6.8, 7.4.13 y 7.2.14; para FortiManager y FortiAnalyzer 8.0.2, 7.6.8, 7.4.12 y 7.2.13; FortiMail 8.0.2 / 7.6.7 / 7.4.9 y FortiAuthenticator 8.0.4 / 6.6.11. [R09]

Fortinet informó que el detalle público de los CVE asociados a este lanzamiento se espera para el 10/11. No corresponde asignar automáticamente un CVE específico o explotación activa a este paquete sin respaldo oficial. Separadamente, existen alertas previas sobre CVE-2025-61624 (FortiOS, entre otros) y vulnerabilidades PSIRT de octubre que requieren inventario propio. [R09]

Acción: preparar backups de configuración, verificar ruta de actualización de cada modelo, restringir la administración por Internet, conservar logs y comprobar cambios de cuentas, túneles VPN, políticas y objetos de seguridad.

4.4. Microsoft Exchange, Authenticator y sistemas Windows

Microsoft Exchange Server CVE-2026-62911 corresponde a una omisión de autenticación por captura/retransmisión, calificada alta (CVSS 8.0), con correcciones lanzadas en agosto de 2026; las evaluaciones de octubre deben centrarse en equipos que siguen sin aplicar actualizaciones o Extended Security Updates cuando corresponda. El vector depende de la versión y del escenario de autenticación. La mera existencia de exploits públicos no demuestra explotación de una instalación. [R10]

CVE-2026-80097 en Microsoft Authenticator fue publicada en septiembre de 2026 como elevación local de privilegios (CVSS 8.6 según registros consultados). En esta revisión no se acreditó un nuevo parche, modificación sustancial ni incorporación a KEV durante el intervalo; debe quedar en seguimiento y

confirmarse su orientación de remediación en el registro MSRC específico, sin atribuirle ejecución remota de código. [R11]

La actualización mensual de Microsoft de octubre, así como CVE-2026-96951 de Windows (incluida en KEV el 13/10), constituyen antecedentes para el control de parches, no novedades originadas el 29–30. Revisar Windows Server, Exchange, endpoints, identidad, RDP, controles MFA, privilegios y registros de correo. [R10]

4.5. Oracle, Java SE y aplicaciones de negocio

La Critical Patch Update del 20/10/2026 contiene 1295 parches nuevos en distintas familias Oracle, entre ellos 55 relacionados con Java SE (49 potencialmente explotables de forma remota sin autenticación en las condiciones descritas por Oracle) y 194 para Oracle E-Business Suite (31 de posible explotación remota sin autenticación). No equivale a afirmar que cada instalación incorpora 1295 CVE ni que todas esas fallas presentan explotación activa. [R12]

Acción: inventariar versiones y componentes Java SE, GraalVM, WebLogic, Oracle Database, Oracle E-Business Suite y librerías empaquetadas. Clasificar por aplicación y exposición, aplicar CPU y pruebas de compatibilidad, renovar servicios dependientes y documentar el parche efectivo. En servicios de terceros, exigir constancia de mantenimiento y resultado de validación.

4.6. IBM Db2 — parches y componentes derivados

IBM registra Security Updates 94236 (Db2 11.5.9), 94722 (Db2 12.1.4) y 94858 (Db2 12.1.5), publicados el 08/10, con correcciones acumulativas para CVE de privilegios, denegación de servicio y componentes federados. CVE-2026-18166 es un ejemplo de carga arbitraria de bibliotecas en el comando CREATE WRAPPER por usuarios privilegiados; CVE-2026-105464 describe escalada local con DBADM y CVE-2026-49844 afecta Log4j en componentes federados. [R14]

Los boletines de Db2 Developer Extension del 26–28/10 tratan CVE-2026-91776 y CVE-2026-91777 (Jackson) y CVE-2026-102276, CVE-2026-102277 y CVE-2026-102278 (brace-expansion), pero no deben confundirse con fallas del motor DB2 general ni clasificarse automáticamente como nacidas en estas 32 horas. [R14]

Acción: determinar el motor exacto (db2level), las extensiones instaladas, las cuentas con DBADM/SYSADM, federación, superficies JDBC/DRDA y los SU instalados. Hacer backup consistente, preservar logs/auditoría y actualizar mediante Fix Central.

4.7. Firefox, Edge, Node.js, PHP y otros componentes

Mozilla lanzó el 27/10 Firefox 159 y avisos correspondientes para Firefox ESR y Thunderbird, con numerosas correcciones relevantes. Son antecedentes previos a esta ventana; se deben desplegar mediante inventario y política de navegadores. Para Microsoft Edge, los parches de Chromium no permiten inferir la compilación exacta ya instalada en cada canal: consultar la nota oficial de Edge y comprobar la versión corporativa real. [R15]

Node.js publicó versiones de seguridad el 21/10 para las ramas 22, 24 y 26, con fallas como CVE-2026-105482 y dependencias (Brotli, Undici, OpenSSL, certificados eMudhra, entre otras). El 28/10 aparecen nuevas versiones 24.22.2 y 26.13.0; no se ha confirmado en esta revisión que constituyan una nueva publicación de seguridad originada dentro de las 32 horas. [R16]

PHP mantiene un programa de versiones de mantenimiento y CVE que también repercute en productos empaquetados; el riesgo concreto debe atribuirse al binario y producto efectivamente afectados. NGINX, Microsoft IIS, WordPress, proveedores cloud, Java de terceros y firmware de routers deben permanecer bajo vigilancia, pero no corresponde listar parches novedosos sin un aviso verificable para este intervalo.

5. Priorización basada en activos críticos

Prioridad	Escenario de exposición	Decisión operativa
P0 / inmediata	Gestión pública de PAN-OS; GitLab expuesto sin parche; Cisco SSL VPN vulnerable; Drupal Commerce explotado.	Aislar administración, preservar evidencia, validar parche y vigilar actividad en paralelo.
P1 / 24 horas	Adobe/Magento vulnerable; ESX/vCenter con cuentas privilegiadas; Fortinet perimetral sin hardening.	Inventario, análisis de compromiso, copia de configuración, actualización controlada.
P2 / 72 horas	Chrome/Firefox/Edge en endpoints; Exchange local; servidores Node/PHP; Oracle/Java/Db2.	Desplegar actualizaciones por oleadas, comprobar versiones, reiniciar cuando corresponda.
P3 / 7 días	Sistemas sin evidencia de instalación afectada; plataformas bajo control de proveedores.	Formalizar respuesta de terceros, excepciones documentadas y remediación programada.

Los plazos anteriores son objetivos operativos orientativos de Instel & Seguridad, no vencimientos impuestos por los fabricantes ni una obligación legal general de Argentina. Las fechas KEV de CISA aplican a organizaciones estadounidenses sujetas al régimen pertinente y se usan aquí como indicador externo de urgencia.

6. Protocolo de verificación y preservación forense

1. Inventario: registrar propietario, servicio, producto, versión completa, compilación/hotfix, fecha de último parche, sistema operativo, dirección IP, exposición pública y responsable.
2. Antes de corregir: si hay señales de compromiso, preservar logs nativos y remotos, artefactos persistentes, usuarios/sesiones, configuración, tareas y metadatos; calcular SHA-256 de los paquetes de evidencia.
3. Visibilidad perimetral: revisar accesos a interfaces MGT, IP de origen, eventos VPN, cambios administrativos, autenticaciones fallidas, túneles, política, certificados y reinicios.
4. Virtualización: correlacionar eventos ESX/vCenter, backup, SIEM, identidad, MFA y hypervisor; conservar evidencia fuera del host.
5. Aplicaciones web: revisar archivos subidos, cambios en CMS/DB, extensiones, web shells, panel admin, claves y llamadas API; limitar bloqueos destructivos hasta preservar evidencia.
6. Aplicación de parches: ejecutar sobre ambiente de prueba cuando sea viable, respaldar configuración, registrar ventana de mantenimiento, hash de artefactos, versión previa/posterior y prueba funcional.
7. Postparche: comprobar que el servicio reinició con versión nueva, revisar alertas, cerrar exposición transitoria, verificar ausencia de persistencia y documentar riesgo residual.

7. Evidencia mínima y pruebas de cumplimiento

Activo	Evidencia recomendada	Control de salida
Navegadores	Listado EDR/MDM/GPO + versión por equipo	Chrome ≥156.0.8078.79 según plataforma; Firefox 159 o ESR corregido.
Fortinet / PAN-OS / Cisco	show version, configuración exportada, backups, logs VPN/MGT	Parche de subrama, plano gestión privado y credenciales revisadas.
VMware	Build ESXi/vCenter, logs remotos, cuenta y MFA	Build conforme VMSA; trazas externas preservadas.
Exchange / Windows	Build, KB/SU y registros de	Actualización instalada y endpoints

Activo	Evidencia recomendada	Control de salida
	actualizaciones	expuestos revisados.
Oracle / Java / IBM Db2	java -version, db2level, inventario aplicativos	CPU/SU por componente y pruebas funcionales.
GitLab / Drupal / Magento	Versiones de aplicación y módulos, hashes, logs web	Rama corregida; evidencia de integridad y accesos revisada.

8. Riesgo de terceros y atribución institucional

Una vulnerabilidad anunciada por un fabricante no implica automáticamente que un organismo o empresa estén comprometidos. El alcance debe surgir de un inventario verificado y una evaluación técnica. Cuando el software vulnerable corresponde a hosting, pasarela de pagos, SaaS, soporte de fabricantes o proveedores externos, el cliente puede no tener potestad para instalar el parche: corresponde exigir una declaración verificable de versión, plan de mitigación, gestión de incidentes y evidencia contractual, en vez de atribuirle indebidamente una omisión técnica.

Por la misma razón, en los informes entregados a direcciones, presidencias y administradores deben distinguirse “afectado comprobado”, “potencialmente afectado”, “no aplicable”, “mitigado” y “pendiente de confirmación del proveedor”. No deben afirmarse exfiltración, ransomware o persistencia sin evidencia informática independiente.

9. Conclusiones y recomendaciones formales

La revisión demuestra que el evento más importante del intervalo no fue una única vulnerabilidad universal, sino la convergencia de actualizaciones de navegadores, inclusión de GitLab y Cisco en KEV, documentación actualizada de ataques sobre PAN-OS y confirmación documental de una vulnerabilidad explotada en Drupal Commerce. El retraso entre publicación del parche y aplicación real continúa siendo la variable principal de exposición. [R01–R06]

Instel & Seguridad recomienda priorizar dispositivos perimetrales, repositorios de desarrollo, virtualización y aplicaciones que procesen pagos o información sensible; completar inventarios y evidencias de mantenimiento, y consolidar una práctica de monitoreo de vulnerabilidades verificable con fuentes primarias. Las tecnologías Microsoft, Fortinet, Oracle/Java, IBM Db2 y navegadores deben integrarse a la misma matriz de gestión de cambios, con responsabilidad explícita por activo y registro de validación del parche.

Se recomienda emitir avisos internos de urgencia para activos P0/P1 y un resumen ejecutivo separado para autoridades, dejando el detalle técnico y la matriz de referencias en este paper. Esta publicación no reemplaza pruebas autorizadas de configuración o análisis forense sobre cada activo.

Referencias oficiales y técnicas consultadas

[R01] Google Chrome Releases — actualización 29/10/2026. https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02107719452.html

[R02] CISA KEV — catálogo de explotación conocida. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[R03] GitLab — parche crítico 21/10 y mantenimiento 29/10. https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/

[R03b] GitLab — releases 19.5.3 y asociadas, sin fixes de seguridad. https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-3-released/

[R04] Cisco — ASA/FTD CVE-2026-76418.
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75

[R05] Palo Alto Networks — CVE-2026-109618/109619. https://security.paloaltonetworks.com/CVE-2026-109618

[R06] Drupal — SA-CONTRIB-2026-254. https://www.drupal.org/sa-contrib-2026-254

[R07] Broadcom — VMSA-2026-0006. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

[R08] Adobe Commerce / Magento — APSB26-73. https://www.adobe.com/trust/security/products/commerce/apsb26-73.html

[R09] Fortinet — hardening release, 21–22/10/2026. https://www.fortinet.com/blog/ciso-collective/fortinet-releases-security-hardening-release-for-multiple-products

[R10] Microsoft Exchange — CVE-2026-62911, verificación CERT gubernamental. https://cert.gov.ng/advisories/microsoft-exchange-server-authentication-bypass-vulnerability

[R11] Microsoft Authenticator — CVE-2026-80097 (registro de seguimiento). https://www.cve.org/CVERecord?id=CVE-2026-80097

[R12] Oracle — Critical Patch Update, octubre de 2026. https://www.oracle.com/security-alerts/cpuoct2026.html

[R13] Palo Alto Networks — Brotli CVE-2026-111497. https://security.paloaltonetworks.com/CVE-2026-111497

[R14] IBM — índice de boletines de Db2 / Security Updates. https://www.ibm.com/support/pages/published-security-vulnerabilities-db2-linux-unix-and-windows-including-security-update-information

[R15] Mozilla Firefox 159 — MFSA 2026-118. https://www.mozilla.org/en-US/security/advisories/mfsa2026-118/

[R16] Node.js — security releases 21/10/2026. https://nodejs.org/en/blog/vulnerability/october-2026-security-releases

[R17] Gobierno de Canadá — VMware, actualización del 28/10. https://www.cyber.gc.ca/en/alerts-advisories/vmware-security-advisory-av26-763

[R18] IBM — Db2 Developer Extension / jackson-databind. https://www.ibm.com/support/pages/security-bulletin-ibm-db2-developer-extension-affected-vulnerability-jackson-databind-cve-2026-91776-cve-2026-91777

[R19] IBM — Db2 Developer Extension / brace-expansion. https://www.ibm.com/support/pages/node/7294579

INSTEL & SEGURIDAD

Fin del documento • Elaboración técnica, sin firma digital ni manuscrita incorporada