CM Carla | SecuMom 

SECUMOM THREAT INTELLIGENCE

Weekly Exposure Brief

04/09/2026

Inteligencia accionable para priorizar la remediación de vulnerabilidades con mayor impacto en el negocio.

For CISOs · Security Managers · SOC Leaders

60	34	10	27
CVES PRIORIZADAS	CAMPAÑAS	CISA KEV	CRÍTICAS

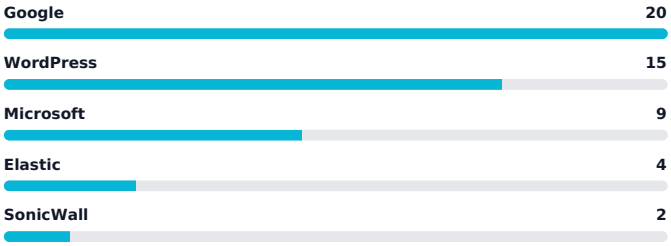
Edición 10 · Generado 2026-09-04 13:11:46 · by Carla Moreno

1. Resumen ejecutivo

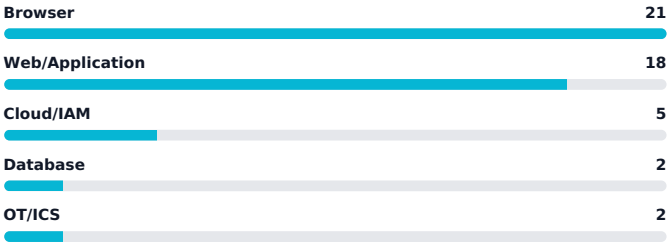
Mensaje clave: las 60 vulnerabilidades priorizadas se agrupan en 34 campañas de remediación. Las vulnerabilidades identificadas esta semana se concentran en pocas campañas de remediación. Priorizar estas acciones permite reducir significativamente la superficie de exposición sin tratar cada CVE de forma aislada.

27	32	10	37	3
CRITICAL	HIGH	CISA KEV	RCE	PUBLIC POC

Top Vendors



Top Technologies



2. Campañas prioritarias de remediación

1

P1

Google Chrome

20 CVEs · 8 críticas · 1 KEV · 20 RCE

131.65
PRIORITY SCORE

CVSS MÁXIMO	EPSS MÁXIMO	SLA RECOMENDADO
9.6	0.46%	24 horas

Plan de remediación: Actualizar Google Chrome a la versión corregida y verificar cobertura en endpoints, VDI y servidores con navegador.

Acción: Confirmar cobertura de actualización y buscar intentos de explotación relacionados con los CVEs incluidos.

CVEs incluidos: CVE-2026-85046 · CVE-2026-85050 · CVE-2026-85047 · CVE-2026-85042 · CVE-2026-84353 · CVE-2026-84352 · CVE-2026-84354 · CVE-2026-84333 · CVE-2026-85051 · CVE-2026-84324 · CVE-2026-84347 · CVE-2026-85053 · CVE-2026-85049 · CVE-2026-84326 · CVE-2026-85048 · CVE-2026-84350 · CVE-2026-84351 · CVE-2026-84349 · CVE-2026-84335 · CVE-2026-84334

2

P1

SonicWall SMA1000

2 CVEs · 1 críticas · 2 KEV · 1 RCE

40.16
PRIORITY SCORE

CVSS MÁXIMO	EPSS MÁXIMO	SLA RECOMENDADO
10.0	1.63%	24 horas

Plan de remediación: Actualizar SMA1000 a una versión corregida y validar su presencia en activos críticos.

Acción: Validar presencia del producto, exposición y eventos anómalos asociados a los CVEs agrupados.

CVEs incluidos: CVE-2026-83549 · CVE-2026-83548

3

P1

PaperCut PaperCut MF/NG

2 CVEs · 1 críticas · 2 KEV · 0 RCE

37.57
PRIORITY SCORE

CVSS MÁXIMO	EPSS MÁXIMO	SLA RECOMENDADO
9.4	1.69%	24 horas

Plan de remediación: Aplicar parches de seguridad, restringir acceso administrativo y validar exposición.

Acción: Validar presencia del producto, exposición y eventos anómalos asociados a los CVEs agrupados.

CVEs incluidos: CVE-2026-82078 · CVE-2026-81578

4

P1

Sangoma Switchvox SMB Edition

1 CVEs · 1 críticas · 1 KEV · 1 RCE

32.48
PRIORITY SCORE

CVSS MÁXIMO	EPSS MÁXIMO	SLA RECOMENDADO
9.3	11.84%	24 horas

Plan de remediación: Actualizar Switchvox SMB Edition a una versión corregida y validar su presencia en activos críticos.

Acción: Validar presencia del producto, exposición y eventos anómalos asociados a los CVEs agrupados.

CVEs incluidos: CVE-2026-9586

5

P1

kestra-io kestra

1 CVEs · 1 críticas · 1 KEV · 1 RCE

32.19
PRIORITY SCORE

CVSS MÁXIMO	EPSS MÁXIMO	SLA RECOMENDADO
10.0	1.92%	24 horas

Plan de remediación: Actualizar la aplicación vulnerable y aplicar controles compensatorios en el WAF hasta completar la remediación.

Acción: Revisar WAF, accesos anómalos y errores asociados al producto vulnerable.

CVEs incluidos: CVE-2026-49869

3. Top vulnerabilidades de la semana

Cada vulnerabilidad se presenta una única vez junto con su contexto de riesgo y acción recomendada. KEV, RCE, PoC y severidad se integran en la misma fila.

#	CVE	Producto	CVSS	EPSS	Indicadores	Acción
1	CVE-2026-9586	Sangoma Switchvox SMB Edition	9.3	11.84%	KEV · RCE · PoC · Critical	Actualizar Switchvox SMB Edition a una versión corregida y validar su presencia en activos críticos.
2	CVE-2026-49869	kestra-io kestra	10.0	1.92%	KEV · RCE · PoC · Critical	Actualizar la aplicación vulnerable y aplicar controles compensatorios en el WAF hasta completar la remediación.
3	CVE-2026-48710	Kludex starlette	6.5	36.26%	KEV · PoC · Medium	Actualizar la aplicación vulnerable y aplicar controles compensatorios en el WAF hasta completar la remediación.
4	CVE-2026-83549	SonicWall SMA1000	7.8	1.63%	KEV · RCE · High	Actualizar SMA1000 a una versión corregida y validar su presencia en activos críticos.
5	CVE-2026-85046	Google Chrome	8.8	0.46%	KEV · RCE · High	Actualizar Google Chrome a la versión corregida y verificar cobertura en endpoints, VDI y servidores con navegador.
6	CVE-2026-82329	jfrog artifactory	9.8	7.67%	KEV · Critical	Actualizar artifactory a una versión corregida y validar su presencia en activos críticos.
7	CVE-2026-82078	PaperCut PaperCut MF/NG	9.4	1.69%	KEV · Critical	Aplicar parches de seguridad, restringir acceso administrativo y validar exposición.
8	CVE-2026-83548	SonicWall SMA1000	10.0	0.71%	KEV · Critical	Actualizar SMA1000 a una versión corregida y validar su presencia en activos críticos.
9	CVE-2026-81578	PaperCut PaperCut MF/NG	8.8	1.62%	KEV · High	Actualizar la aplicación vulnerable y aplicar controles compensatorios en el WAF hasta completar la remediación.
10	CVE-2026-59822	BerriAI litellm	8.8	0.87%	KEV · High	Actualizar litellm a una versión corregida y validar su presencia en activos críticos.
11	CVE-2026-70352	Microsoft Azure	10.0	0.62%	Critical	Aplicar el parche del proveedor y revisar recursos, privilegios y actividad anómala asociada.
12	CVE-2026-83711	Microsoft Azure	10.0	0.58%	Critical	Aplicar el parche del proveedor y revisar recursos, privilegios y actividad anómala asociada.
13	CVE-2026-72649	Elastic Elasticsearch	8.8	0.58%	RCE · High	Actualizar Elasticsearch a una versión corregida y validar su presencia en activos críticos.
14	CVE-2026-63137	Elastic Kibana	8.3	0.33%	High	Actualizar Kibana a una versión corregida y validar su presencia en activos críticos.
15	CVE-2026-78583	Elastic Kibana	8.1	0.20%	High	Actualizar Kibana a una versión corregida y validar su presencia en activos críticos.

4. Acciones recomendadas para esta semana

1. Confirmar cobertura de actualización y buscar intentos de explotación relacionados con los CVEs incluidos.
2. Validar presencia del producto, exposición y eventos anómalos asociados a los CVEs agrupados.
3. Validar presencia del producto, exposición y eventos anómalos asociados a los CVEs agrupados.
4. Validar presencia del producto, exposición y eventos anómalos asociados a los CVEs agrupados.
5. Revisar WAF, accesos anómalos y errores asociados al producto vulnerable.

5. Principales Hallazgos

▲ **Elevada criticidad semanal**

27 de 60 vulnerabilidades priorizadas son críticas (45%). La ejecución debe enfocarse en activos expuestos y tecnologías presentes en servicios esenciales.

◆ **Explotación confirmada**

Se identificaron 10 vulnerabilidades incluidas en CISA KEV. La explotación confirmada exige prioridad incluso cuando no existe una prueba de concepto pública.

◎ **Concentración del riesgo**

El 33% de las vulnerabilidades priorizadas se concentra en Google Chrome. Una sola campaña de remediación cubre 20 CVEs.

▣ **Infraestructura industrial**

12 vulnerabilidades afectan tecnologías asociadas a entornos industriales u OT. La remediación debe coordinarse con operación, disponibilidad y ventanas de mantenimiento.

6. Decisión ejecutiva recomendada

Acciones prioritarias:

- Actualizar Google Chrome a la versión corregida y verificar cobertura en endpoints, VDI y servidores con navegador.
- Actualizar SMA1000 a una versión corregida y validar su presencia en activos críticos.
- Aplicar parches de seguridad, restringir acceso administrativo y validar exposición.
- Actualizar Switchvox SMB Edition a una versión corregida y validar su presencia en activos críticos.

Una vez ejecutadas estas acciones, el riesgo residual deberá gestionarse según la criticidad de los activos afectados, la exposición del servicio y la presencia real de cada tecnología en el entorno.