GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4326

2026-11-10 · semana del 04/11/2026 al 10/11/2026

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido al boletín semanal del CSOC-CERT de Gamma Ingenieros. Aquí encontrará, en pocas páginas, lo que más importa para proteger a su organización esta semana: las vulnerabilidades que hay que corregir ya, el malware más activo, lo que se movió en los medios y cómo se están atacando las organizaciones en Colombia y Panamá. Cada tema trae enlaces y recomendaciones concretas.

EN ESTA EDICIÓN

> Esta semana el foco está en Linux kernel, Microsoft y OpenSSH: las fallas ya se explotan en ataques reales, así que la recomendación es actualizar sin esperar a la ventana de mantenimiento. En malware, XMRig fue la familia con más actividad reportada. En Colombia y Panamá registramos 21 organizaciones afectadas en el último mes, con la administración pública como el sector más golpeado.

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	56	415	0
MALWARE	0	2	2
NOTICIAS DE CIBERSEGURIDAD	0	0	6

Vulnerabilidades: todas las de severidad alta o crítica, o ya explotadas, publicadas en la semana en el mundo para las tecnologías que vigilamos (471). Más adelante detallamos las más relevantes.

Organizaciones afectadas o reclamadas por actores de amenaza esta semana:

7
en Colombia y Panamá

20
en el resto de Latinoamérica

337
en el resto del mundo

21
en Colombia y Panamá, últimos 30 días

VULNERABILIDADES

Estas son las fallas que recomendamos atender primero. Empezamos por las tecnologías que Gamma distribuye y seguimos por riesgo real: las que ya se están explotando y luego las de mayor severidad.

FORTINET: 52 VULNERABILIDADES ESTA SEMANA (11 CRÍTICAS)

¿Qué pasó?

Esta semana se publicaron 52 vulnerabilidades de severidad alta o crítica, o ya explotadas, en Fortinet: 11 críticas. Los tipos de falla más frecuentes son recorrido de directorios (path traversal), inyección de

comandos del sistema operativo e inyección SQL. La de mayor prioridad es FG-IR-26-199 (recorrido de directorios (path traversal), CVSS 9.8).

¿Por qué importa?

Permite leer o dejar archivos donde no se debe, por ejemplo configuraciones con contraseñas o código malicioso. Es una tecnología presente en muchas de las organizaciones que acompañamos.

Datos técnicos:

- Vulnerabilidades de la semana: 52 (11 críticas).
- Las de mayor prioridad: FG-IR-26-199 (recorrido de directorios (path traversal), CVSS 9.8); FG-IR-26-200 (inyección de comandos, CVSS 9.8); CVE-2026-121529 (CVSS 9.6); FG-IR-26-216 (inyección SQL, CVSS 9.4); FG-IR-26-267 (CVSS 9.3) y 47 más.
- Puntaje más alto: CVSS 9.8.
- Explotación: sin ataques reportados al cierre de esta edición.

¿Qué hacer?

1. Actualice Fortinet a la versión corregida que indica el fabricante (enlaces al final).
2. Revise si hay archivos nuevos o modificados en los directorios web y cambie las contraseñas que puedan haber quedado expuestas.
3. Confirme con un escaneo que no queden equipos con versiones vulnerables.

Prioridad: Crítica.

Para ampliar:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-199
- https://fortiguard.fortinet.com/psirt/FG-IR-26-200
- https://nvd.nist.gov/vuln/detail/CVE-2026-121529

LINUX KERNEL: 4 VULNERABILIDADES ESTA SEMANA (1 CRÍTICA)

¿Qué pasó?

Esta semana se publicaron 4 vulnerabilidades de severidad alta o crítica, o ya explotadas, en Linux kernel: 1 crítica y 1 ya explotada en ataques reales. El tipo de falla más frecuente es autorización incorrecta. La de mayor prioridad es CVE-2026-123218 (autorización incorrecta, CVSS 9.8, ya explotada).

¿Por qué importa?

Ya se está usando en ataques reales, así que cada día sin parche cuenta. Un usuario puede ver o modificar lo que no le corresponde, y desde ahí escalar.

Datos técnicos:

- Vulnerabilidades de la semana: 4 (1 crítica, 1 ya explotada en ataques reales).

- Las de mayor prioridad: CVE-2026-123218 (autorización incorrecta, CVSS 9.8, ya explotada); CVE-2026-100081 (CVSS 7.8); CVE-2026-99281 (CVSS 7.8); CVE-2026-99277 (CVSS 7.5).
- Puntaje más alto: CVSS 9.8.
- Explotación: confirmada en ataques reales para CVE-2026-123218 (catálogo KEV de CISA).

¿Qué hacer?

1. Actualice Linux kernel a la versión corregida que indica el fabricante (enlaces al final).
2. Revise qué usuarios tienen acceso al producto y retire los permisos que no se usan.
3. Parchear no basta si el atacante ya entró: busque usuarios, tareas programadas o archivos que nadie reconozca en los equipos afectados.
4. CISA fijó para las entidades federales de EE. UU. un plazo hasta el 12 de noviembre; tómelo como referencia máxima.
5. Confirme con un escaneo que no queden equipos con versiones vulnerables.

Prioridad: Crítica.

Para ampliar:

- https://nvd.nist.gov/vuln/detail/CVE-2026-123218
- https://nvd.nist.gov/vuln/detail/CVE-2026-100081
- https://nvd.nist.gov/vuln/detail/CVE-2026-99281
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

---

MICROSOFT: 276 VULNERABILIDADES ESTA SEMANA (12 CRÍTICAS)

¿Qué pasó?

Esta semana se publicaron 276 vulnerabilidades de severidad alta o crítica, o ya explotadas, en Microsoft: 12 críticas y 2 ya explotadas en ataques reales. Los tipos de falla más frecuentes son desbordamiento de búfer en el montículo (heap), uso de memoria ya liberada y desbordamiento de búfer en la pila. La de mayor prioridad es CVE-2026-125350 (uso de memoria ya liberada, CVSS 8.8, ya explotada).

¿Por qué importa?

Los atacantes ya la están aprovechando: hay que tratarla como una urgencia. Es una falla de memoria: en el mejor caso tumba el servicio y en el peor permite ejecutar código del atacante.

Datos técnicos:

- Vulnerabilidades de la semana: 276 (12 críticas, 2 ya explotadas en ataques reales).
- Las de mayor prioridad: CVE-2026-125350 (uso de memoria ya liberada, CVSS 8.8, ya explotada); CVE-2026-124194 (CVSS 6.5, ya explotada); CVE-2026-120002 (autorización incorrecta, CVSS 9.9); CVE-2026-116928 (escritura fuera de los límites de memoria, CVSS 9.8); CVE-2026-95882 (desbordamiento de búfer en la pila, CVSS 9.8) y 271 más.
- Puntaje más alto: CVSS 9.9.

- Explotación: confirmada en ataques reales para CVE-2026-125350 y CVE-2026-124194 (catálogo KEV de CISA).

¿Qué hacer?

1. Actualice Microsoft a la versión corregida que indica el fabricante (enlaces al final).
2. Si no puede actualizar hoy, reduzca la exposición del servicio y active la protección de exploits del EDR.
3. Revise los registros de los últimos días en los equipos expuestos; si ve accesos o procesos que no reconoce, trate el caso como un incidente.
4. CISA fijó para las entidades federales de EE. UU. un plazo hasta el 24 de noviembre; tómelo como referencia máxima.
5. Confirme con un escaneo que no queden equipos con versiones vulnerables.

Prioridad: Crítica.

Para ampliar:

- https://nvd.nist.gov/vuln/detail/CVE-2026-125350
- https://nvd.nist.gov/vuln/detail/CVE-2026-124194
- https://nvd.nist.gov/vuln/detail/CVE-2026-120002
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

---

OPENSSH: VULNERABILIDAD ALTA (CVE-2026-123158)

¿Qué pasó?

Se publicó una vulnerabilidad de severidad alta en OpenSSH. CISA confirmó que ya se está explotando desde el 9 de noviembre.

¿Por qué importa?

CISA confirmó ataques reales con esta falla.

Datos técnicos:

- Identificador: CVE-2026-123158.
- Severidad: Alta (CVSS 8.1).
- Explotación: confirmada en ataques reales (catálogo KEV de CISA, desde el 9 de noviembre).
- Probabilidad de explotación en los próximos 30 días (FIRST EPSS): 16 %.

¿Qué hacer?

1. Actualice OpenSSH a la versión corregida que indica el fabricante (enlaces al final).
2. Antes de dar el caso por cerrado, confirme con el EDR o el SIEM que no hubo actividad sospechosa en esos equipos.
3. CISA fijó para las entidades federales de EE. UU. un plazo hasta el 12 de noviembre; tómelo como referencia máxima.
4. Confirme con un escaneo que no queden equipos con versiones vulnerables.

Prioridad: Crítica.

Para ampliar:

- https://nvd.nist.gov/vuln/detail/CVE-2026-123158
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

---

SONICWALL: 4 VULNERABILIDADES ESTA SEMANA (1 YA EXPLOTADA EN ATAQUES REALES)

¿Qué pasó?

Esta semana se publicaron 4 vulnerabilidades de severidad alta o crítica, o ya explotadas, en SonicWall: 1 ya explotada en ataques reales. El tipo de falla más frecuente es desbordamiento de búfer en el montículo (heap). La de mayor prioridad es CVE-2026-19868 (CVSS 7.5, ya explotada).

¿Por qué importa?

No es un riesgo teórico: ya hay atacantes aprovechándola.

Datos técnicos:

- Vulnerabilidades de la semana: 4 (1 ya explotada en ataques reales).
- Las de mayor prioridad: CVE-2026-19868 (CVSS 7.5, ya explotada); CVE-2026-107154 (CVSS 8.8); CVE-2026-107155 (CVSS 8.8); CVE-2026-82308 (desbordamiento de búfer en el montículo (heap), CVSS 7.5).
- Puntaje más alto: CVSS 8.8.
- Explotación: confirmada en ataques reales para CVE-2026-19868 (catálogo KEV de CISA).

¿Qué hacer?

1. Actualice SonicWall a la versión corregida que indica el fabricante (enlaces al final).
2. Como ya se está explotando, revise también si el equipo fue comprometido antes del parche: cuentas o tareas nuevas, procesos extraños y conexiones salientes inusuales.
3. CISA fijó para las entidades federales de EE. UU. un plazo hasta el 20 de noviembre; tómelo como referencia máxima.
4. Confirme con un escaneo que no queden equipos con versiones vulnerables.

Prioridad: Crítica.

Para ampliar:

- https://nvd.nist.gov/vuln/detail/CVE-2026-19868
- https://nvd.nist.gov/vuln/detail/CVE-2026-107154
- https://nvd.nist.gov/vuln/detail/CVE-2026-107155
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

---

TOP 10 DE FABRICANTES Y TECNOLOGÍAS DE LA SEMANA

Las marcas con más vulnerabilidades relevantes en la semana, empezando por las que Gamma distribuye. Si usa alguna, revise sus avisos de seguridad y aplique las actualizaciones.

FABRICANTE O TECNOLOGÍA	VULNERABILIDADES	CRÍTICAS	YA EXPLOTADAS	CVSS MÁS ALTO	TIPOS DE FALLA MÁS FRECUENTES
Fortinet	52	11	—	9.8	Recorrido de directorios (path traversal), inyección de comandos del sistema operativo, inyección SQL
Illumio	2	0	—	7.8	—
Microsoft	276	12	2	9.9	Desbordamiento de búfer en el montículo (heap), uso de memoria ya liberada, desbordamiento de búfer en la pila
Barracuda Networks	2	0	2	—	Inyección de comandos del sistema operativo, omisión de autenticación
Linux kernel	4	1	1	9.8	Autorización incorrecta
Apple	3	1	1	9.1	Autenticación indebida, validación indebida de certificados
SonicWall	4	0	1	8.8	Desbordamiento de búfer en el montículo (heap)
Cisco	1	0	1	—	—
GPUStack	1	0	1	—	Autenticación indebida
OpenSSH	1	0	1	8.1	—

MALWARE

Las familias de malware con más actividad reportada por la comunidad de inteligencia en los últimos siete días, qué hacen y cómo protegerse.

XMRIG

¿Qué pasó?

XMRig es una familia de malware o herramienta usada en ataques. Esta semana aparece en 5 informes de inteligencia publicados en AlienVault OTX, con 129 indicadores asociados y 76 técnicas de ataque (MITRE ATT&CK) descritas.

¿Por qué importa?

Está entre las familias más nombradas en los informes de la semana: conviene confirmar que sus controles la detectan.

¿Qué hacer?

1. Revise los informes enlazados y cargue sus indicadores en el firewall, el proxy y el EDR.
2. Busque hacia atrás (últimos 30 días) conexiones a esos indicadores en los registros de DNS, proxy y EDR.

Prioridad: Urgente.

Para ampliar:

- https://otx.alienvault.com/pulse/6af1ef5821afddb68d6df42b
- https://otx.alienvault.com/pulse/6ac84a1665712fe245b07ce7
- https://otx.alienvault.com/pulse/6ac7794a227de27b373a9281

ARTEX

¿Qué pasó?

ARTEX es una familia de malware o herramienta usada en ataques. Esta semana aparece en 5 informes de inteligencia publicados en AlienVault OTX, con 39 indicadores asociados y 50 técnicas de ataque (MITRE ATT&CK) descritas.

¿Por qué importa?

Está entre las familias más nombradas en los informes de la semana: conviene confirmar que sus controles la detectan.

¿Qué hacer?

1. Revise los informes enlazados y cargue sus indicadores en el firewall, el proxy y el EDR.
2. Busque hacia atrás (últimos 30 días) conexiones a esos indicadores en los registros de DNS, proxy y EDR.

Prioridad: Urgente.

Para ampliar:

- https://otx.alienvault.com/pulse/6af22c74c56e69bb42cb8363
- https://otx.alienvault.com/pulse/6aeeb5bc2f487ae6d84ea7e9
- https://otx.alienvault.com/pulse/6ac8a22f8d0ad1ea5f056ddc

DARKSWORD

¿Qué pasó?

DarkSword es una familia de malware o herramienta usada en ataques. Esta semana aparece en 3 informes de inteligencia publicados en AlienVault OTX, con 53 indicadores asociados y 28 técnicas de ataque (MITRE ATT&CK) descritas.

¿Por qué importa?

Está entre las familias más nombradas en los informes de la semana: conviene confirmar que sus controles la detectan.

¿Qué hacer?

1. Revise los informes enlazados y cargue sus indicadores en el firewall, el proxy y el EDR.
2. Busque hacia atrás (últimos 30 días) conexiones a esos indicadores en los registros de DNS, proxy y EDR.

Prioridad: Importante.

Para ampliar:

- https://otx.alienvault.com/pulse/6ac6bb9cd16a3898ced29ead
- https://otx.alienvault.com/pulse/6aebe661b7e5525aa39d6ba8
- https://otx.alienvault.com/pulse/6aeb242026030af6a32b4b10

XWORM

¿Qué pasó?

XWorm es un troyano de acceso remoto (RAT). Esta semana aparece en 2 informes de inteligencia publicados en AlienVault OTX, con 92 indicadores asociados y 20 técnicas de ataque (MITRE ATT&CK) descritas.

¿Por qué importa?

Está entre las familias más nombradas en los informes de la semana: conviene confirmar que sus controles la detectan.

¿Qué hacer?

1. Revise los informes enlazados y cargue sus indicadores en el firewall, el proxy y el EDR.
2. Busque hacia atrás (últimos 30 días) conexiones a esos indicadores en los registros de DNS, proxy y EDR.

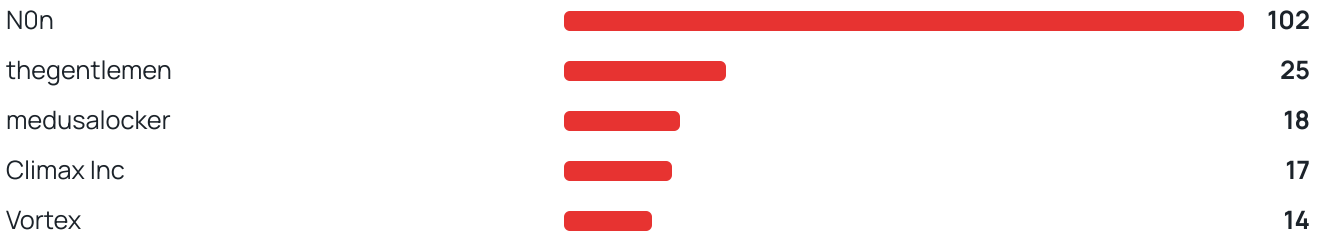
Prioridad: Importante.

Para ampliar:

- https://otx.alienvault.com/pulse/6aeb242105ebdc46e55850e9
- https://otx.alienvault.com/pulse/6ac34ecea12957741eb7ac1b

RANSOMWARE: LA SEMANA EN NÚMEROS

Esta semana, 364 organizaciones aparecieron publicadas en los sitios donde los grupos de ransomware exhiben a sus víctimas. Estos fueron los grupos más activos en el mundo:



qilin 13

Lo que pasó en Colombia y Panamá lo contamos en la sección de tendencias.

Fuente: ransomware.live. Que un grupo reclame un ataque no lo confirma por sí solo.

Recomendaciones generales contra el malware:

1. Mantenga actualizados sus sistemas y priorice las vulnerabilidades que ya se están explotando.
2. Active la autenticación multifactor (MFA) en correo, VPN y cuentas con privilegios.
3. Desconfíe de correos, mensajes y enlaces inesperados: el phishing sigue siendo la principal puerta de entrada.
4. Mantenga copias de seguridad que no se puedan borrar ni cifrar desde la red, y pruebe que puede restaurarlas.
5. Dé a cada usuario solo los permisos que necesita y revise los accesos de sus proveedores.

NOTICIAS DE CIBERSEGURIDAD

Lo que se publicó esta semana en medios y que vale la pena leer:

- **La Inteligencia Artificial amplía la superficie de riesgo: los nuevos desafíos de ciberseguridad para las empresas colombianas**
  ITSitio · 5 de noviembre · Leer la nota
- **INAC presente en el Simulacro de Ciberseguridad Aeronáutica organizado por la Autoridad Aeronáutica de Colombia**
  Ministerio del Poder Popular para el Transporte (MPPT) · 5 de noviembre · Leer la nota
- **¿Pueden hackear su nevera en Colombia? El ciberataque en Europa que puso en alerta a los hogares con electrodomésticos inteligentes**
  El Tiempo · 5 de noviembre · Leer la nota
- **Ciberataque en el Pico y Placa Solidario de Bogotá puso en riesgo el dinero y los datos de los usuarios: Secretaría de Movilidad respondió | El Colombiano**
  El Colombiano · 5 de noviembre · Leer la nota
- **Plataforma de Pico y Placa Solidario en Bogotá sufrió un ciberataque que pondría en peligro el dinero de los usuarios: esto dijo la Secretaría de Movilidad**
  Infobae · 5 de noviembre · Leer la nota
- **“No soy conspiranoico”: Westcol compra provisiones para un año por temor a un ciberataque**
  Colombia.com · 4 de noviembre · Leer la nota

Titulares de medios públicos seleccionados por el CSOC-CERT; el contenido de cada nota es responsabilidad del medio.

TENDENCIAS DE ATAQUE EN EL MUNDO Y EN LATINOAMÉRICA

Esta semana registramos 357 organizaciones afectadas o reclamadas por actores de amenaza fuera de Colombia y Panamá: 20 en el resto de Latinoamérica (11 en Brasil, 6 en México, 1 en Argentina, 1 en Chile y 1 en Venezuela) y 337 en el resto del mundo, repartidas en 37 países.

Conteos tomados de lo que publican los propios atacantes y de fuentes públicas; un reclamo no confirma por sí solo un ataque.

TENDENCIAS DE ATAQUE EN COLOMBIA Y PANAMÁ

En los últimos 30 días contamos 21 organizaciones de la región afectadas o reclamadas por actores de amenaza (17 en Colombia y 4 en Panamá), sube 17 % frente al mes anterior; 7 casos en la última semana.

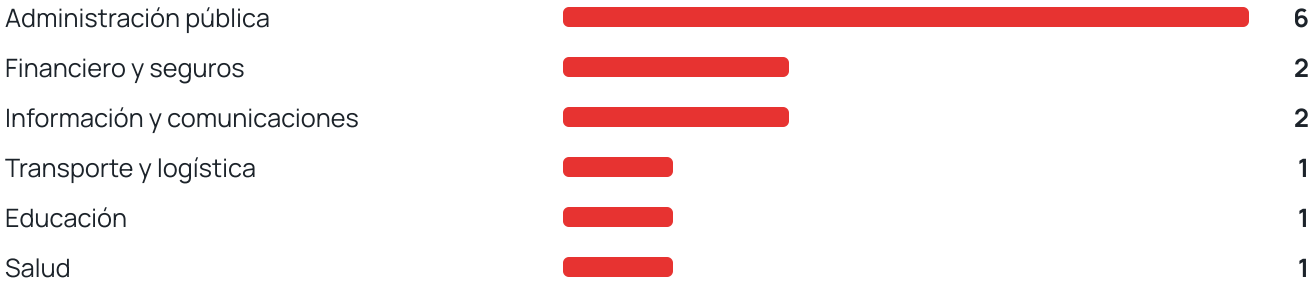
El sector más golpeado fue la administración pública, con 6 casos, seguido de financiero y seguros (2), información y comunicaciones (2) y transporte y logística (1).

Ransomware sigue siendo la amenaza principal (9 casos, baja 25 % frente al mes anterior), y le sigue phishing y suplantación (6).

Los grupos con más reclamos en la región fueron emperador (2), thegentlemen (2) y terroah (1).

7 de estos casos ya están confirmados por la víctima, una autoridad o un medio; el resto se basa en lo que publica el propio atacante, que no siempre es cierto, pero sí es una señal para revisar.

SECTORES MÁS AFECTADOS (ÚLTIMOS 30 DÍAS)



Además, 8 casos quedaron sin sector identificado.

CÓMO ATACAN



Ojo con la cadena de suministro: en el mismo periodo, 5 proveedores o multinacionales con operación en la región también fueron víctimas (software empresarial (erp/saas), industria y ot y consumo

masivo). Un incidente en un proveedor puede llegar a sus clientes: si trabaja con uno de este tipo, pregúntele si se vio afectado y revise los accesos que tiene a su red.

Qué hacer según su sector:

- **Administración pública:** Haga inventario de los portales expuestos a internet, parchee primero las vulnerabilidades ya explotadas (KEV), active MFA en correo y VPN, y vigile la desfiguración de sus sitios .gov.co.
- **Financiero y seguros:** Use MFA resistente a phishing, vigile las credenciales de sus empleados expuestas por infostealers y controle los accesos de terceros (core, pagos, BPO).
- **Información y comunicaciones:** Revise la cadena de suministro de su software, rote las llaves de API y vigile los accesos privilegiados de sus clientes.
- **Transporte y logística:** Proteja los portales de clientes y de rastreo, exija MFA en los accesos remotos y respalde los sistemas de operación.

Gamma CSOC-CERT: su aliado en ciberseguridad

Las amenazas de este boletín cambian cada semana. El Centro de Operaciones de Ciberseguridad y equipo de respuesta (CSOC-CERT) de Gamma Ingenieros vigila estas amenazas por usted y le ayuda a actuar a tiempo.

- Inteligencia de amenazas para Colombia y Panamá: ransomware, filtraciones, infostealers y campañas activas.
- Alertas tempranas de vulnerabilidades críticas del portafolio de su organización.
- Gestión de vulnerabilidades y priorización según explotación activa (CISA KEV, EPSS).
- Acompañamiento en la respuesta a incidentes y en la recuperación.

¿Quiere saber si su organización está expuesta? Contacte a su ejecutivo de cuenta de Gamma Ingenieros.

https://gammaingenieros.com

Fuentes de esta edición: CISA KEV, NVD, FIRST EPSS, avisos de fabricantes, ThreatFox (abuse.ch), ransomware.live, Google Noticias y el monitoreo del CSOC-CERT de Gamma Ingenieros. Periodo: 2026-11-04 a 2026-11-10. Información pública · TLP:GREEN.