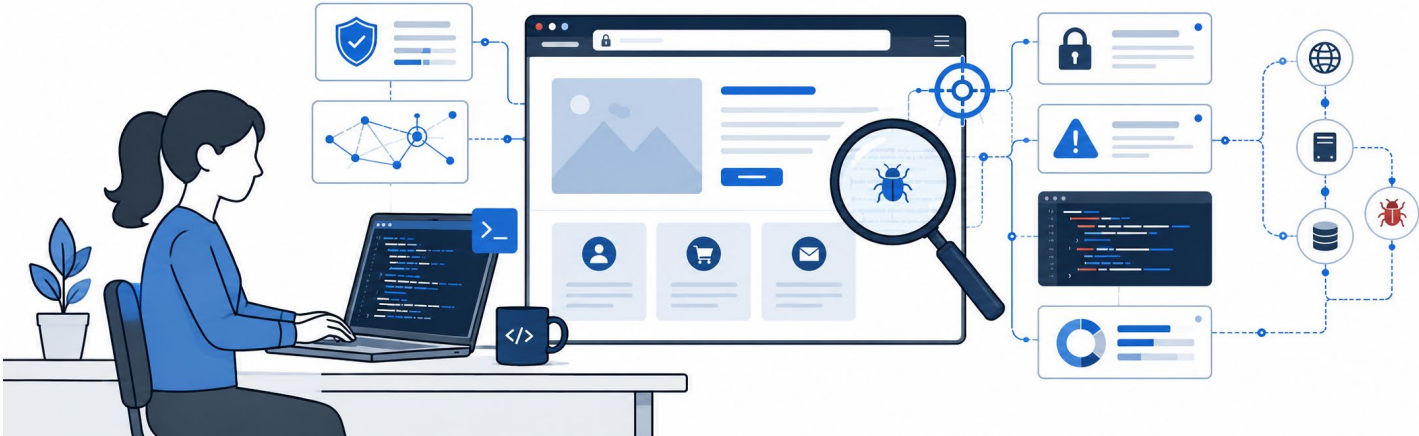


Vulnerabilidades identificadas en el primer semestre de 2026



A continuación se indican los datos cuantitativos y cualitativos de las vulnerabilidades identificadas en el primer semestre de 2026, de modo que permitan evaluar la situación actual y la tendencia para este año. En el informe se destacan las vulnerabilidades que han tenido especial relevancia durante el período mencionado.

Se incluyen aquellas que están siendo activamente explotadas y las que están relacionadas con familias de ransomware con mayor número de víctimas. Estos hallazgos resaltan la importancia de implementar políticas de actualizaciones y de gestión de vulnerabilidades con el objetivo de minimizar el riesgo de ser afectado por su explotación.



35.494

Vulnerabilidades publicadas
▲ +61,70% vs S1 2025 (21.950→35.494)

2.538

Fabricantes afectados
▲ +107,01% vs S1 2025 (1.226→2.538)

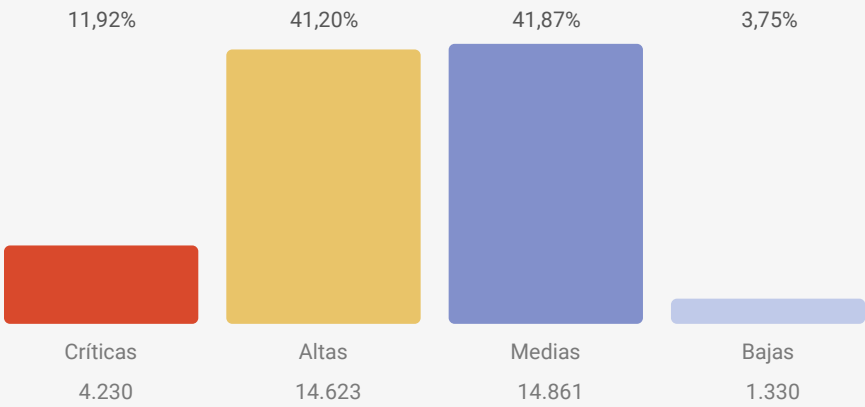
1.639

Explotadas activamente (total)
▲ +18,68% vs S1 2025 (1.381→1.639)

146

Nuevas en explotación activa
▲ +9,77% vs S1 2025 (133→146)

Distribución por severidad



* 450 vulnerabilidades no tienen severidad asignada (CVSS pendiente)

Top 10 fabricantes

Por número de vulnerabilidades identificadas

1	Linux	3.082	33%
2	Microsoft	1.681	18%
3	Google	1.291	14%
4	Apple	1.213	13%
5	Openclaw	447	5%
6	Oracle	441	5%
7	IBM	300	3%
8	Apache	296	3%
9	Adobe	275	3%
10	Tenda	258	3%

Top 10 productos

Por número de vulnerabilidades identificadas

1	Linux Kernel	3.082	36%
2	MacOS	1.147	14%
3	Windows	1.053	12%
4	Chrome	1.008	12%
5	Openclaw	447	5%
6	Android	396	5%
7	Windows Server 2025	342	4%
8	Windows 11 24H2	332	4%
9	Windows 11 25H2	331	4%
10	Windows Server 2022 23H2	323	4%

Vulnerabilidades activamente explotadas

1.639

Total vulnerabilidades explotadas acumuladas
▲ +18,68% incremento del total acumulado vs S1 2025 (1.381→1.639)

146

Nuevas vulnerabilidades en explotación activa en S1 2026
▲ +9,77% incremento de nuevas explotadas vs S1 2025 (133→146)

Top 10 vulnerabilidades según el software afectado

Distribución de vulnerabilidades activamente explotadas por categoría

Sistema operativo		21	21,64%
Gestión IT		15	15,46%
Networking		8	8,24%
Productos de seguridad		8	8,24%
Ofimática		7	7,21%
Sistemas de correo		6	6,18%
Servicios cloud		6	6,18%
Buscadores		5	5,15%
Infraestructura		5	5,15%
Herramientas web		3	3,09%
Otros		13	13,40%

Top 5 fabricantes-productos con vulnerabilidades activamente explotadas

FABRICANTE	PRODUCTOS	CANT.
Microsoft	Windows (11), Office (4), Defender (3), Internet Explorer (2), Configuration Manager (1)	21
Cisco	Catalyst SD-WAN Manager (4), Unified Communications Manager (2), Catalyst SD-WAN (1), Catalyst SD-WAN Controller (1)	8
Apple	Multiple Products (6), iOS and iPadOS (1)	7
Google	Chromium V8 (2), Chromium (1), Dawn (1), Skia (1)	5
Ivanti	Endpoint Manager Mobile EPMM (3), Endpoint Manager EPM (1), Sentry (1)	5

Vulnerabilidades explotadas por las familias de ransomware más activas en el primer semestre de 2026



Qilin 1.121 víctimas 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy 9.6 CVE-2024-21762 Fortinet FortiOS 9.3 CVE-2026-50751 Check Point VPN 9.3 CVE-2025-5777 Citrix NetScaler ADC/GW 8.8 CVE-2024-1708 ConnectWise ScreenConnect 7.5 CVE-2023-27532 Veeam Backup & Replication	Thegentlemen 710 víctimas 10.0 CVE-2026-20131 Cisco Secure Firewall FMC (RCE) 10.0 CVE-2025-32433 Erlang/OTP SSH 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy 9.3 CVE-2026-50751 Check Point Security GW 8.8 CVE-2025-33073 Windows SMB/Kerberos Relay	Akira 533 víctimas 9.3 CVE-2024-40766 SonicWall SonicOS SSL VPN 9.1 CVE-2023-20269 Cisco ASA 7.5 CVE-2020-3259 Cisco AnyConnect 7.5 CVE-2023-27532 Veeam Backup & Replication	Dragonforce 425 víctimas 9.8 CVE-2024-57726/27/28 SimpleHelp RMM 9.3 CVE-2025-5777 Citrix NetScaler (CitrixBleed 2) 8.2 CVE-2023-46805 Ivanti Connect Secure 5.5 CVE-2025-61155 Tower of Fantasy driver	Incransom 425 víctimas 9.8 CVE-2023-3519 Citrix NetScaler ADC/Gateway
NightSpire 351 víctimas 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy	Lockbit5 326 víctimas 9.8 CVE-2023-27350 PaperCut MF/NG 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy 9.3 CVE-2023-0669 Fortra GoAnywhere MFT	Play 288 víctimas 9.8 CVE-2020-12812 Fortinet SSL VPN 9.8 CVE-2024-57727 SimpleHelp RMM 9.1 CVE-2018-13379 Fortinet FortiOS 8.8 CVE-2022-41040 Microsoft Exchange 8.8 CVE-2022-41080 Microsoft Exchange 8.0 CVE-2022-41082 Microsoft Exchange RCE 7.8 CVE-2025-29824 Microsoft Windows CLFS	Clop 256 víctimas 9.8 CVE-2024-50623 Cleo (carga/descarga) 9.3 CVE-2023-0669 GoAnywhere MFT 9.1 CVE-2023-34362 MOVEit Transfer SQL injection 9.1 CVE-2024-55956 Cleo RCE 9.1 CVE-2021-27101/02/03/04 Accellion FTA	CoinBase Cartel 224 víctimas Sin CVEs atribuidas públicamente

CVE-2024-55591 (FortiOS/FortiProxy · CVSS 9.8 crítica) — la vulnerabilidad más compartida del semestre: presente en al menos 4 de los 10 grupos más activos (Qilin, Thegentlemen, NightSpire y Lockbit5). Incluida en el catálogo CISA KEV.

Conclusiones

- 1

Crecimiento exponencial: ruptura de la tendencia moderada. Las vulnerabilidades publicadas alcanzan 35.494 (+61,70% vs S1 2025), rompiendo el crecimiento moderado del año anterior (+5,05%). Los fabricantes afectados más que duplican: 2.538 vs 1.226 en 2025.
- 2

Agravamiento severo de la criticidad. Críticas + Altas saltan del 18,11% al 53,12% — más de la mitad del total. Las críticas prácticamente se duplican (6,58%→11,92%) y las altas casi se cuadruplican (11,53%→41,20%).
- 3

Linux, Microsoft y Google lideran el incremento. Linux Kernel: 876→3.082 (+252%). Microsoft: 377→1.681 (+346%). Google irrumpe con 1.291 vulnerabilidades desde una presencia casi residual en 2025 (109).
- 4

Explotación activa: crecimiento sostenido. El total con explotación activa alcanza 1.639 (+18,68% vs 1.381 en S1 2025); 146 nuevas incorporaciones (+9,77% vs 133). Sistemas operativos concentran el 21,64%, seguidos de gestión IT (15,46%). Microsoft lidera con 21 vulnerabilidades explotadas, seguido de Cisco (8), Apple (7), Google (5) e Ivanti (5).
- 5

Perímetro como vector crítico en ransomware. Las CVEs explotadas por grupos ransomware se concentran en conectividad (Fortinet, Cisco, Citrix, Check Point), backup (Veeam) y transferencia de archivos y RMM (GoAnywhere, MOVEit, Cleo, SimpleHelp).
- 6

Doble patrón en arsenales de grupos ransomware. Reutilización histórica: CVE-2018-13379, CVE-2020-3259 y CVE-2021-27101/104 siguen activas en 2026. Aceleración del time-to-exploit: CVE-2025-32433 y CVE-2026-20131 aparecen en el mismo semestre de su publicación.

Recomendaciones

- Parcheo priorizado por riesgo real

Basar la priorización en explotación activa confirmada (CISA KEV), no en CVSS puro. Plazo máximo 48-72h para críticas en perímetro.
- Reducción de exposición de perímetro

Auditar VPNs, firewalls, RMM, plataformas de transferencia de archivos y backup accesibles desde internet.
- Monitorización reforzada

Linux (+252%), Microsoft (+346%) y Google (+1.084%) lideran el incremento de vulnerabilidades publicadas. Aplicar hardening donde el parcheo inmediato no sea viable.
- Inteligencia de amenazas contextualizada

Correlacionar vulnerabilidades con actividad de grupos ransomware para anticipar vectores antes de su explotación masiva.
- Formación y concienciación

El incremento en ofimática y correo refuerza la necesidad de formación continua como complemento al parcheo técnico.
- Planes de respuesta acelerados

El time-to-exploit se acorta a horas. Los planes de respuesta deben contemplar compromisos en menos de 24h desde publicación.

Predicciones

- Volumen sin precedentes

La inteligencia artificial aplicada al descubrimiento de vulnerabilidades hace que el total anual se prevea que superará las 70.000 vulnerabilidades por primera vez.
- Severidad sostenida

La proporción de críticas y altas se mantendrá por encima del 50%, consolidando el nuevo estándar de severidad.
- Linux y cloud como focos

Linux Kernel y los entornos cloud seguirán siendo los principales focos de vulnerabilidades por volumen.
- Explotación de perímetro

Los grupos ransomware continuarán explotando CVEs en Fortinet, Cisco y Citrix en las primeras horas tras su publicación, especialmente cuando afectan a dispositivos de conectividad.