Vulnerabilidades 2023
Primer semestre

A continuación, se indican los datos cuantitativos y cualitativos de las vulnerabilidades identificadas en el primer semestre de 2023 que se han identificado, de modo que permita evaluar la situación actual y tendencia en cuanto a las vulnerabilidades surgidas y que son habitualmente utilizadas por los atacantes para llevar a cabo sus ataques.

En el informe se destacan la presencia de varias vulnerabilidades durante el período mencionado, incluyendo aquellas que están siendo activamente explotadas y las que están relacionadas con familias de ransomware de más actividad en este periodo. Estos hallazgos resaltan la importancia de disponer de una política de actualizaciones con el objetivo de minimizar el riesgo a verse afectado por su explotación.

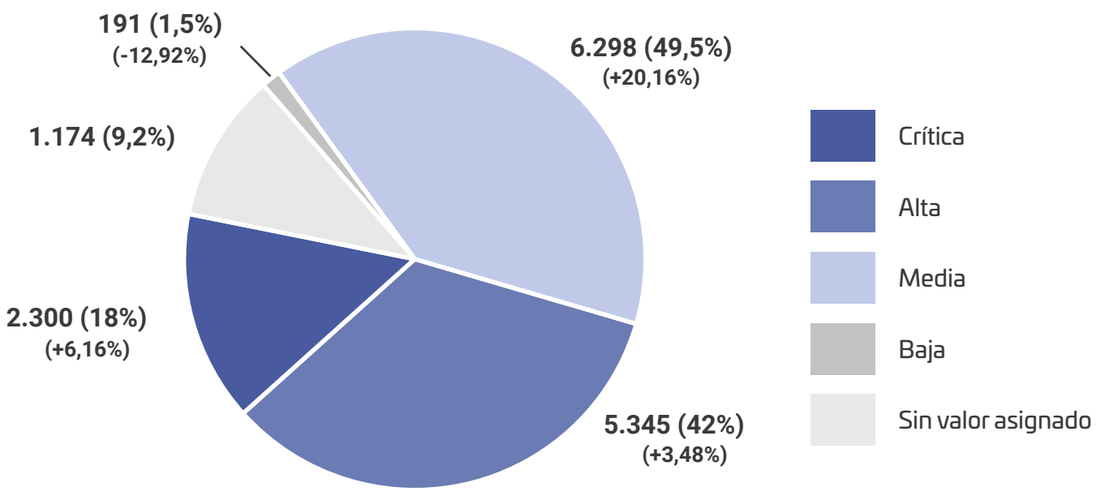
Totales

15.308

Incremento con respecto al año anterior

20,13%

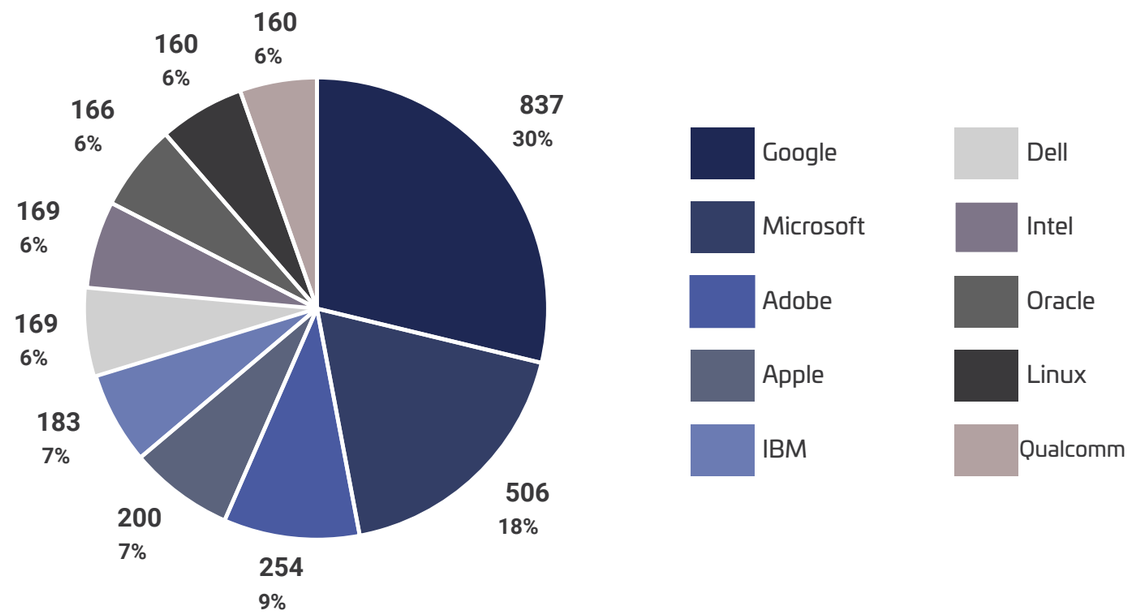
Distribución de vulnerabilidades por severidad



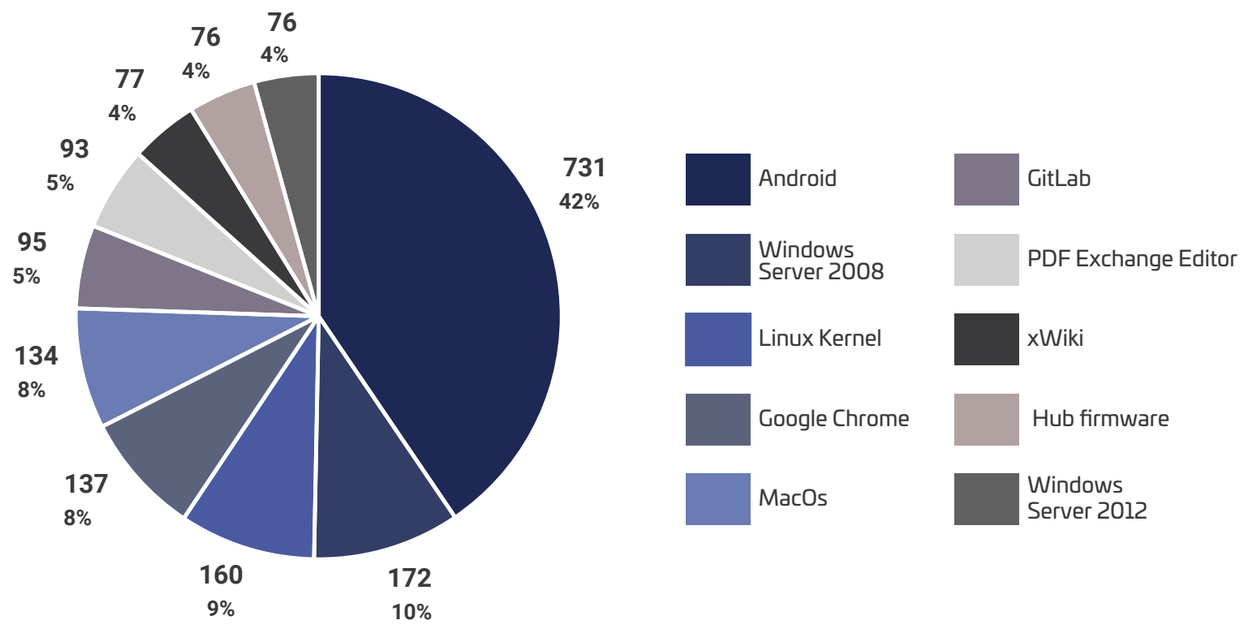
Top 10 CWE (Common Weakness Enumeration)

CWE 79	Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)
CWE 89	Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)
CWE 787	Out-of-bounds Write
CWE 125	Out-of-bounds Read
CWE 352	Cross-Site Request Forgery (CSRF)
CWE 22	Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
CWE 862	Missing Authorization
CWE 20	Improper Input Validation
CWE 77	Improper Neutralization of Special Elements used in a Command (‘Command Injection’)
CWE 120	Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow)

Top 10 fabricantes con vulnerabilidades identificadas



Top 10 productos con vulnerabilidades identificadas



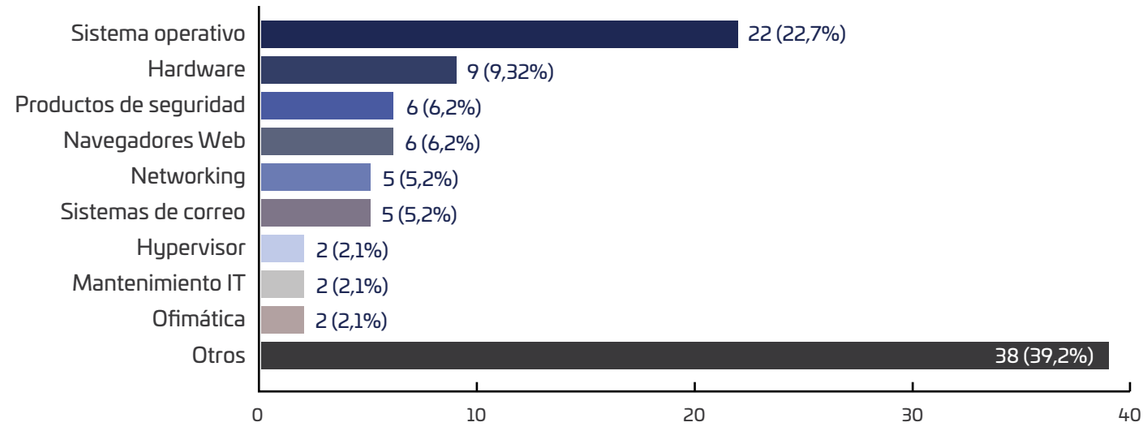
Vulnerabilidades nuevas activamente explotadas de manera masiva

Total de vulnerabilidades explotadas	Vulnerabilidades nuevas	Incremento respecto al año anterior
965	97	11,19%

Top 5 fabricantes-productos con vulnerabilidades activamente explotadas

Fabricante	Productos	Cantidad
Microsoft	Exchange Server Internet Explorer Office Win32k Windows	12
Apple	iOS and macOS iOS, iPadOS and macOS macOS Multiple Products	11
Samsung	Mobile Devices	7
Google	Chrome Chromium V8 Engine	4
Zyxel	Multiple Firewalls Multiple Network-Attached Storage (NAS) Devices	4

Distribución de vulnerabilidades activamente explotadas según el tipo de sistema afectado



Vulnerabilidades explotadas por familias de ransomware más activas en el semestre

Lockbit: 530 víctimas

- CVE-2021-44228 – (10.0 crítica): Apache
- CVE-2020-1472 – (10.0 crítica): Microsoft
- CVE-2018-13379 – (9.8 crítica): Fortinet
- CVE-2023-27350 – (9.8 crítica): Papercut
- CVE-2021-22986 – (9.8 crítica): F5
- CVE-2019-0708 – (9.8 crítica): Microsoft
- CVE-2023-27351 – (7.5 alta): Papercut
- CVE-2023-0669 – (7.2 alta): GoAnywhere

BianLian: 177 víctimas

- CVE-2022-27510 – (9.8 crítica): Citrix

Clop: 137 víctimas

- CVE-2023-34362 – (9.8 crítica): MOVEit
- CVE-2023-27350 – (9.8 crítica): Papercut
- CVE-2023-27351 – (7.5 alta): Papercut
- CVE-2023-0669 – (7.2 alta): GoAnywhere

Royal: 119 víctimas

- CVE-2022-27510 – (9.8 crítica): Citrix

Play: 118 víctimas

- CVE-2022-41080 – (9.8 crítica): Microsoft
- CVE-2022-41082 – (8.8 alta): Microsoft

Nokoyawa: 26 víctimas

- CVE-2023-28252 – (7.8 alta): Microsoft

cyber zaintza