Vulnerabilidades 2023
Informe anual

A continuación, se indican los datos cuantitativos y cualitativos de las vulnerabilidades identificadas en 2023, de modo que permita evaluar la situación actual y tendencia en cuanto a la utilización de las mismas por parte de parte de los ciberdelincuentes.

En el informe se incluyen aquellas que están siendo activamente explotadas y las utilizadas por las familias de ransomware de mayor actividad durante este periodo. Es de vital importancia disponer de una política de actualizaciones para minimizar el riesgo a verse afectado por su explotación.

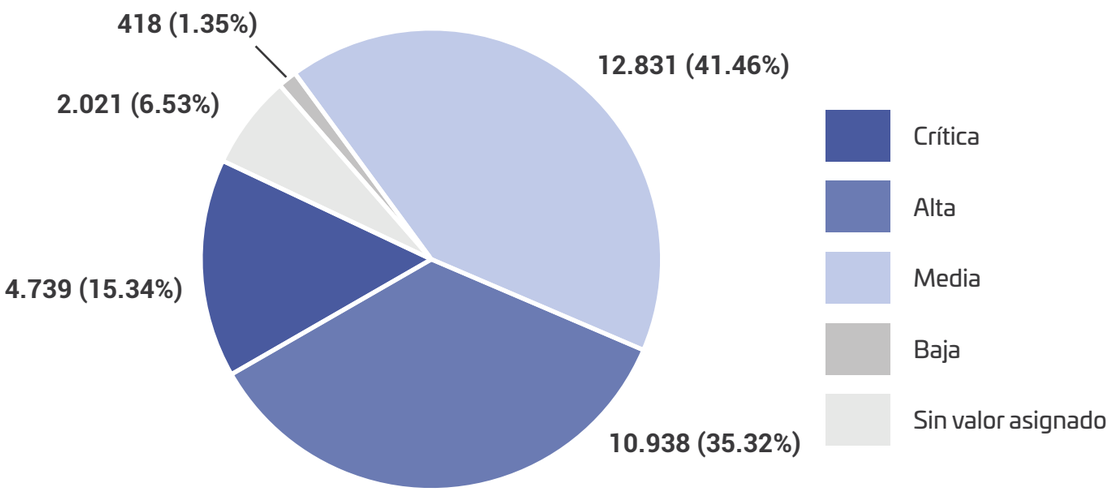
Totales

30.947

Incremento con respecto al año anterior

17.03%

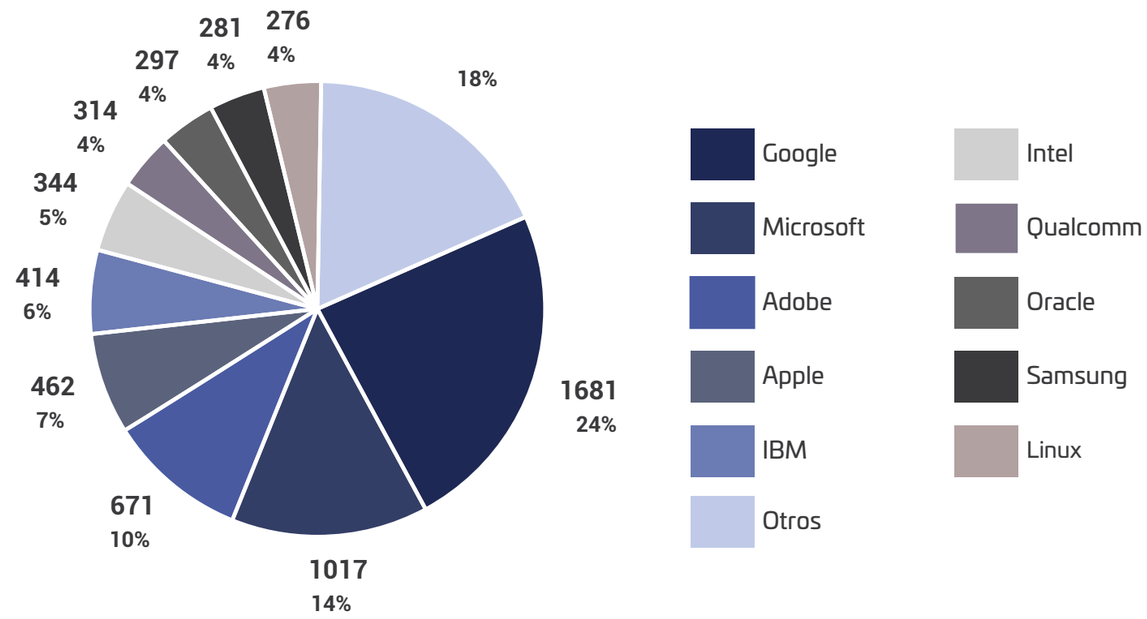
Distribución de vulnerabilidades por severidad



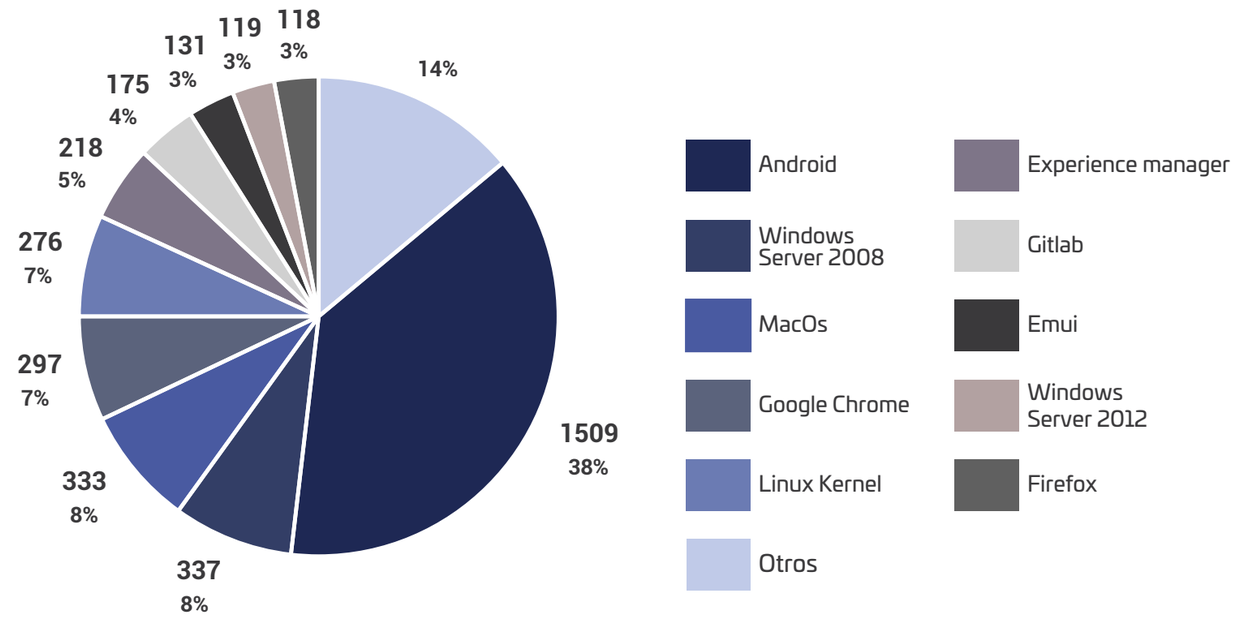
Top 10 CWE (Common Weakness Enumeration)

CWE 79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE 352	Cross-Site Request Forgery (CSRF)
CWE 22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE 120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow)
CWE 77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE 94	Improper Control of Generation of Code ('Code Injection')
CWE 502	Deserialization of Untrusted Data
CWE 269	Improper Privilege Management
CWE 601	URL Redirection to Untrusted Site ('Open Redirect')
CWE 284	Improper Access Control

Top 10 fabricantes con vulnerabilidades identificadas



Top 10 productos con vulnerabilidades identificadas



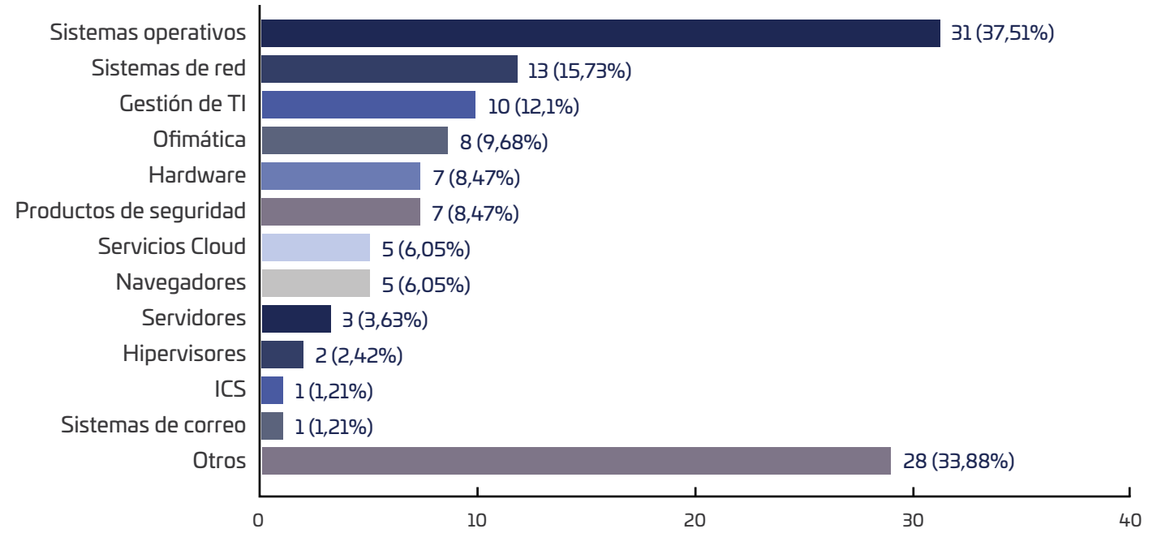
Vulnerabilidades nuevas activamente explotadas de manera masiva

Total de vulnerabilidades explotadas	Vulnerabilidades nuevas	Incremento respecto al año anterior
1.053	121	21,29%

Top 5 fabricantes-productos con vulnerabilidades activamente explotadas

Fabricante	Productos	Cantidad
Apple	iOS, iPadOS and watchOS iOS and iPadOS iOS, iPadOS and macOS Multiple Products	19
Microsoft	Skype for Business Outlook .NET Core and Visual Studio Office Windows	18
Adobe	Acrobat and Reader ColdFusion	6
Google	Skia Chromium webP Chrome libvpx Chrome Chromium V8 Engine	6
Juniper	Junos OS	5

Distribución de vulnerabilidades activamente explotadas según el tipo de sistema afectado



Vulnerabilidades explotadas por familias de ransomware más activas en el semestre

Lockbit3: 1045 víctimas

- CVE 2023-4966: (9.4 crítica)- Citrix Bleed
- CVE-2023-27351: (8.2 Alta)- PaperCut
- CVE-2023-27350: (9.8 crítica)- Papercut
- CVE-2023-0669: (7.2 Alta)- Fortra GoAnywhere MFT

Alphv: 451 víctimas

- CVE-2021-27878: (8.8 Alta) - Veritas Backup
- CVE-2021-27877: (8.2 Alta) - Veritas Backup
- CVE-2021-27876: (8.1 Alta) - Veritas Backup

Clop: 375 víctimas

- CVE-2023-34362: (9.8 crítica)- MOVEit
- CVE-2023-27350: (9.8 crítica)- Papercut
- CVE-2023-27351: (8.2 Alta)- PaperCut
- CVE-2023-0669: (7.2 Alta)- Fortra GoAnywhere MFT

Play : 305 víctimas

- CVE-2020-12812: (9.8 crítica)- FortiOS
- CVE-2022-41080: (9.8 crítica)- Microsoft Exchange Server
- CVE-2018-13379: (9.1 crítica)- FortiOS
- CVE-2022-41040: (8.8 Alta)- Microsoft Exchange Server
- CVE-2022-41082: (8.8 alta)- Microsoft Exchange Server
- CVE-2022-41082: (8.0 Alta)- Microsoft Exchange Server

Bianlian: 284 víctimas

- CVE-2022-27510: (9.8 crítica)- Citrix
- CVE-2020-1472: (5.0 Media)- protocolo Netlogon)

8base: 274 víctimas

- CVE-2017-11882: (7.8 Alta) - Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, y Microsoft Office 2016

Akira: 173 víctimas

- CVE-2023-27532: (7.5 Alta)- Veeam Backup & Replication
- CVE-2023-20269: (5.0 Media)-Cisco

Medusa: 150 víctimas

- CVE-2022-2294: (8.8 Alta)- Google Chrome
- CVE-2022-2295: (8.8 Alta)- Google Chrome
- CVE-2022-21999: (7.8 Alta)- Windows Print Spooler
- CVE-2018-13379: (9.1 crítica)- FortiOS y FortiProxy

Noescape: 123 víctimas

- CVE-2021-34473: (9.1 crítica)- Microsoft Exchange Server
- CVE-2021-34523: (9.0 crítica)- Microsoft Exchange Server
- CVE-2021-31207: (6.6 Media)- Microsoft Exchange Server

Royal: 120 víctimas

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