2023ko ahaltasunak
Urterko txostena

Ziberkriminaleen ahaltasunen erabilera eta joera ebaluatzeko aukera izan dezan, jarraian, 2023an identifikatutako ahultasunen datu kuantitatiboak eta kualitatiboak adierazten dira.

Txostenak, aldi honetan aktiboki ustiatzen ari diren ahaltasunak eta ransomware familiek erabiltzen dituzten ahaltasunak biltzen ditu.
Eragiteko arriskua gutxitzeko, eguneratze- politika izatea oso garrantzitsua da.

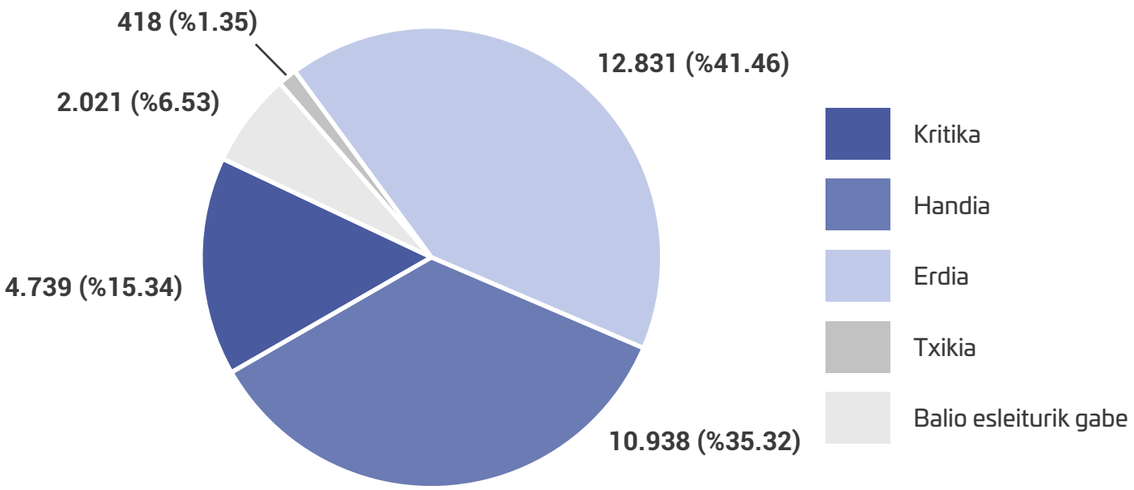
Guztira

30.947

Aurreko urteari dagokionez gehikuntza

%17.03

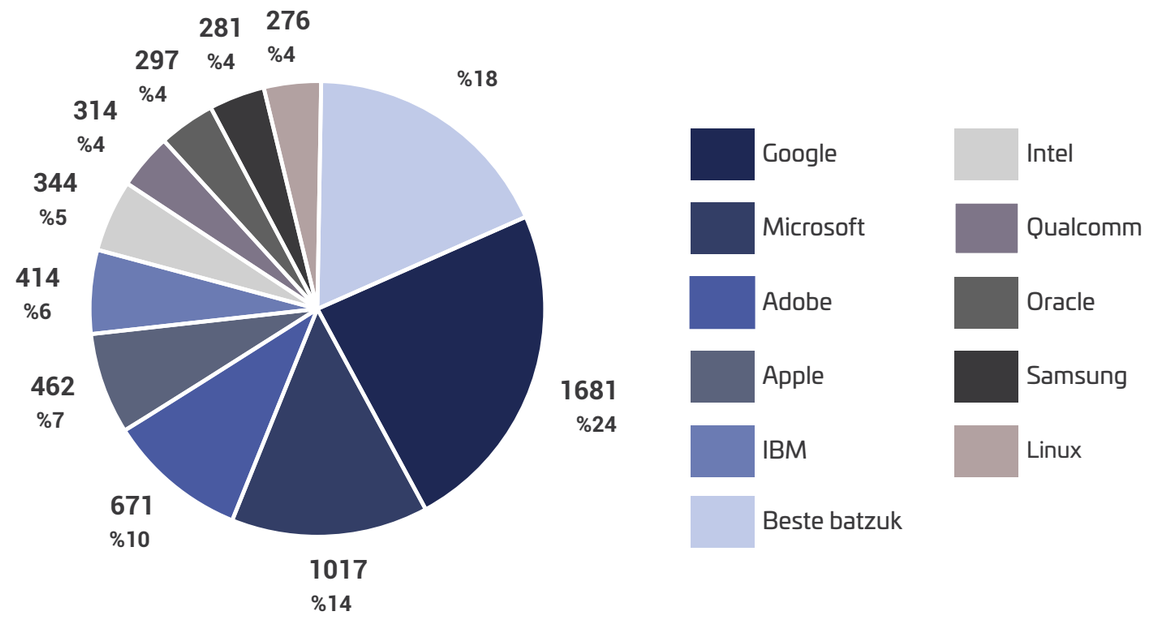
Larritasunaren arabera, ahultasunen sailkapena



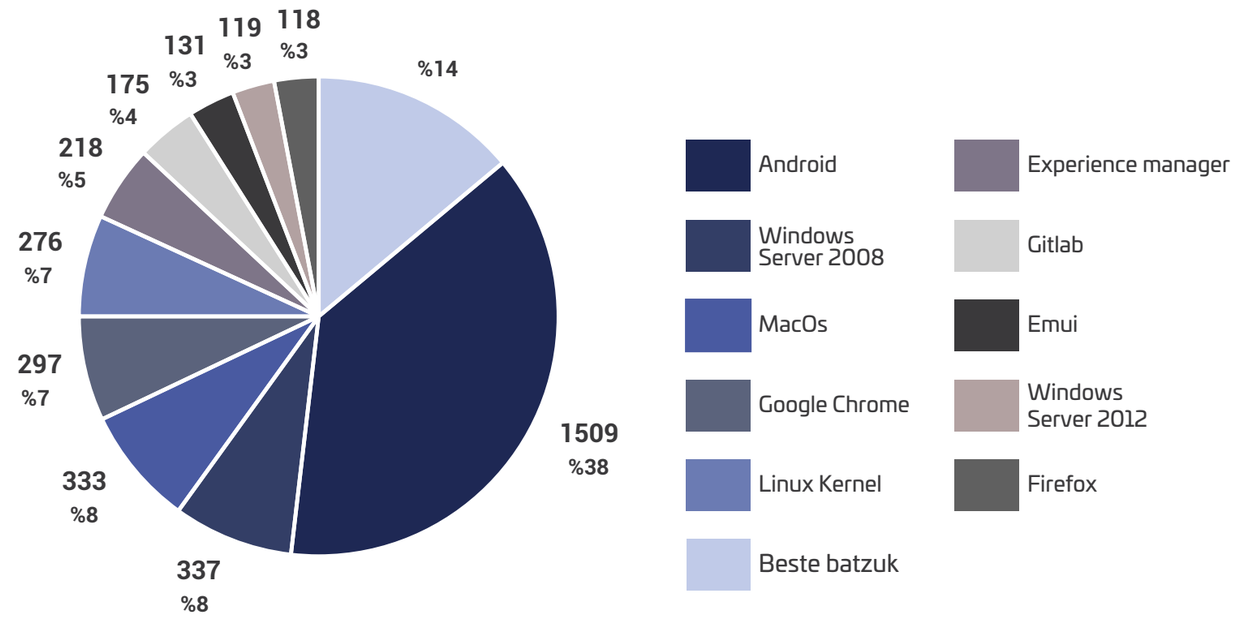
Top 10 CWE (Common Weakness Enumeration)

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

Ahultasunak identifikatuta dituzten 10 fabrikatzaile onenak



Ahultasunak identifikatutako 10 produktu onenak



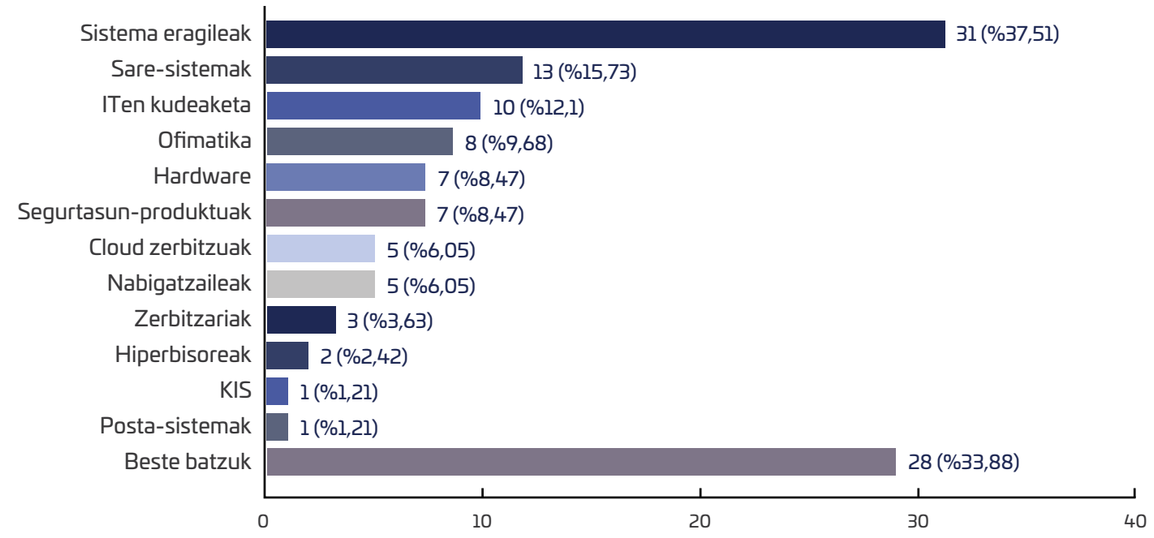
Modu masiboan ustiatutako ahultasun berriak

Ustiatutako ahultasun guztiak	Ahultasun berriak	Aurreko urteari dagokionez gehikuntza
1.053	121	%21,29

Modu aktiboan ustiatutako ahultasunak dituzten produktuen 5 fabrikatzaile onenak

Fabrikatzailea	Produktuak	Produktuak
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

Modu aktiboan ustiatutako ahultasunen banaketa, eragindako sistema-motaren arabera



Seihileko honetan ransomware-familia aktiboenek ustiatutako ahultasunak

Lockbit3: 1045 biktima

- 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 biktima

- 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 biktima

- 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 biktima

- 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 biktima

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

8base: 274 biktima

- 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 biktima

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

Medusa: 150 biktima

- 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 biktima

- 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 biktima

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