2024ko ahaltasunak
Urteko txostena

Jarraian, 2024an identifikatutako kalteberatasunen datu kuantitatiboak eta kualitatiboak ageri dira, eta, horri esker, egungo egoera ebaluatu eta 2025erako aurreikuspenak egin ditzakegu.
Aipatutako aldian zehar bereziki garrantzitsuak izan diren kalteberatasunak nabarmentzen dira txostenean, aktiboki ustiatzen ari direnak eta biktimen kopururik handiena duten ransomware-familiekin lotutakoak barne. Aurkikuntza horiek agerian uzten dute kalteberatasunak eguneratzeko eta kudeatzeko politikak ezartzea zer garrantzitsua den, ustiapenek kalteak eragitea minimizatzeko.

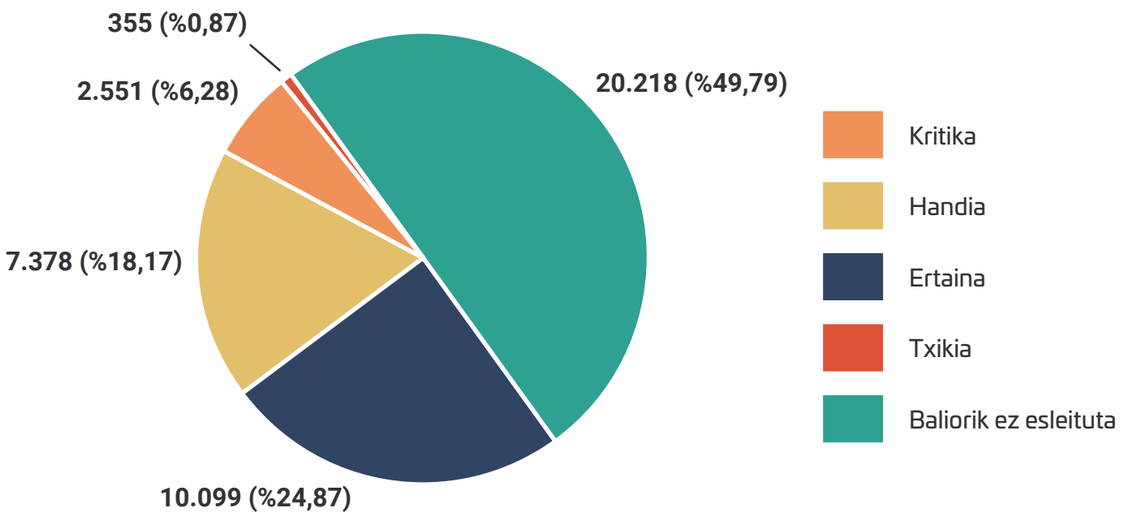
Guztira

40.601

Aurreko urteari dagokionez gehikuntza

%31,21

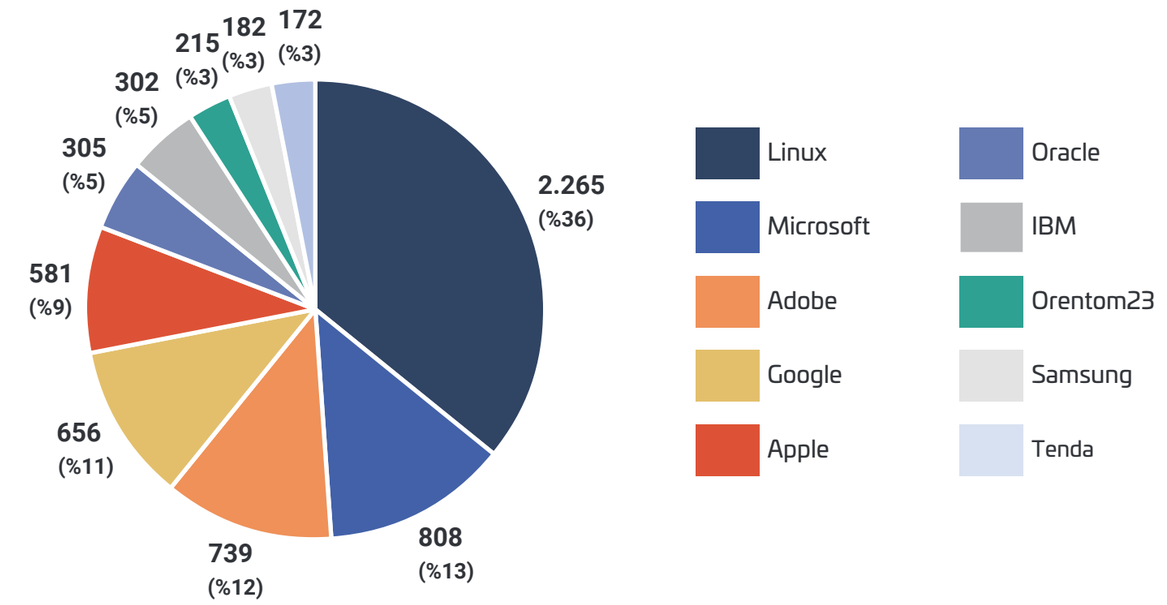
Larritasunaren arabera, ahultasunen sailkapena



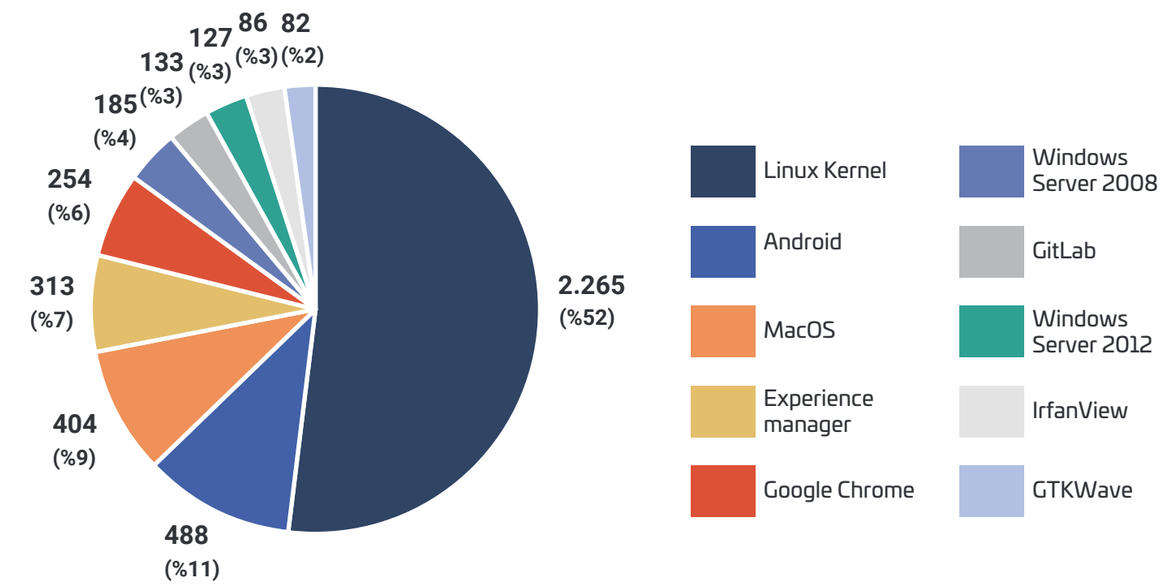
Top 10 CWE (Common Weakness Enumeration)

- **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 862** Missing Authorization
- **CWE 787** Out-of-bounds Write
- **CWE 352** Cross-Site Request Forgery (CSRF)
- **CWE 416** Use After Free
- **CWE 476** NULL Pointer Dereference
- **CWE 125** Out-of-bounds Read
- **CWE 22** Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
- **CWE 434** Unrestricted Upload of File with Dangerous Type

Identifikatutako kalteberatasunen fabrikatzaileen Top 10a



Identifikatutako kalteberatasunen produktuen Top 10a



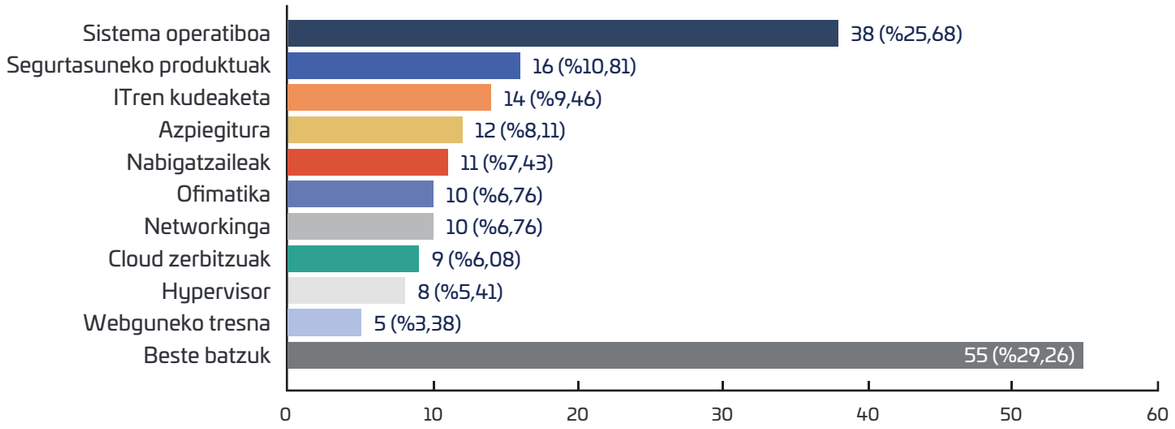
Modu masiboan ustiatutako ahultasun berriak

Ustiatutako ahultasun guztiak	Ahultasun berriak	Aurreko urteari dagokionez gehikuntza
1.239	188	%55,37

Aktiboki ustiatutako kalteberatasunen fabrikatzaileen-produktuen top 5

Fabrikatzailea	Produktuak	Kantitatea
Microsoft	Windows Exchange Server SharePoint Server Internet Explorer DWM Core Library	30
Ivanti	Cloud Services Appliance (CSA) Connect Secure and Policy Secure Cloud Services Appliances Connect Secure, Policy Secure, and ... Endpoint Manager (EPM)	8
Google	Chromium V8 Chromium Chromium Visuals Chromium WebRTC	9
Adobe	Flash Player ColdFusion Commerce and Magneto Open Source	8
Apple	Multiple Products	7

Modu aktiboan ustiatutako ahultasunen banaketa, eragindako sistema-motaren arabera



Urte horretako ransomware familiarik aktiboenek ustiatutako kalteberatasunak

Ransomhub: 632 biktima

- CVE-2020-1472 – (10.0 kritikoa) Microsoft

Lockbit3: 552 biktima

- CVE-2021-22986 – (9.8 kritikoa) F5
- CVE-2023-27350: (9.8 kritikoa)- Papercut
- CVE-2023-4966 (Citrix Bleed) – (9.4 kritikoa) Citrix
- CVE 2023-4966: (9.4 kritikoa)- Citrix
- CVE-2023-27351: (8.2 handia)- PaperCut
- CVE-2023-0669: (7.2 handia)- Fortra GoAnywhere MFT

Play: 367 biktima

- CVE-2020-12812 – (9.8 kritikoa) Fortinet
- CVE-2018-13379 – (9.1 kritikoa) Fortinet
- CVE-2022-41040 (8.8 handia) Microsoft
- CVE-2022-41080 – (8.8 handia) Microsoft
- CVE-2022-41082 -(8.0 handia) Microsoft

Akira: 345 biktima

- CVE-2023-20269 – (9.1 kritikoa) Cisco
- CVE-2020-3259- (7.5 handia) Cisco
- CVE-2023-27532: (7.5 handia)- Veeam Backup & Replication

Hunters: 235 biktima

- CVE-2021-34473 – (9.1 kritikoa) Microsoft
- CVE-2021-34523 – (9.0 kritikoa) Microsoft
- CVE-2021-34527 – (8.8 handia) Microsoft
- CVE-2019-7481 – (7.5 handia) SonicWall
- CVE-2021-31207 – (6.6 ertaina) Microsoft

Medusa: 222 biktima

- CVE-2023-48788 – (9.8 kritikoa) Fortinet
- CVE-2018-13379 – (9.1 kritikoa) Fortinet
- CVE-2022-2294 – (8.8 handia) Google
- CVE-2022-2295 – (8.8 handia) Google
- CVE-2022-21999 – (7.8 handia) Microsoft

Qlin: 189 biktima

- CVE-2023-27532 – (7.5 handia) Veeam Backup & Replication

BlackBasta: 185 biktima

- CVE-2024-1709- (10.0 kritikoa) ConnectWise ScreenConnect
- CVE-2020-1472 – (10.0 kritikoa) Micosoft
- CVE-2021-34527 - (8.8 handia) Microsoft
- CVE-2024-1708 - (8.4 handia) ConnectWise ScreenConnect
- CVE-2024-26169 – (7.8 handia) Microsoft
- CVE-2022-30190 - (7.8 handia) Microsoft

BianLian: 169 biktima

- CVE-2020-1472 – (10.0 kritikoa) Netlogon Remote Protocol

Disposessor: 352 biktima

- Ez da identifikatu ahultasun zehatzen ustiapena.