

Jarraian, 2025ean identifikatutako kalteberatasunen datu kuantitatiboak eta kualitatiboak ageri dira, eta, horri esker, egungo egoera ebaluatu eta 2026rako aurreikuspenak egin ditzakegu.

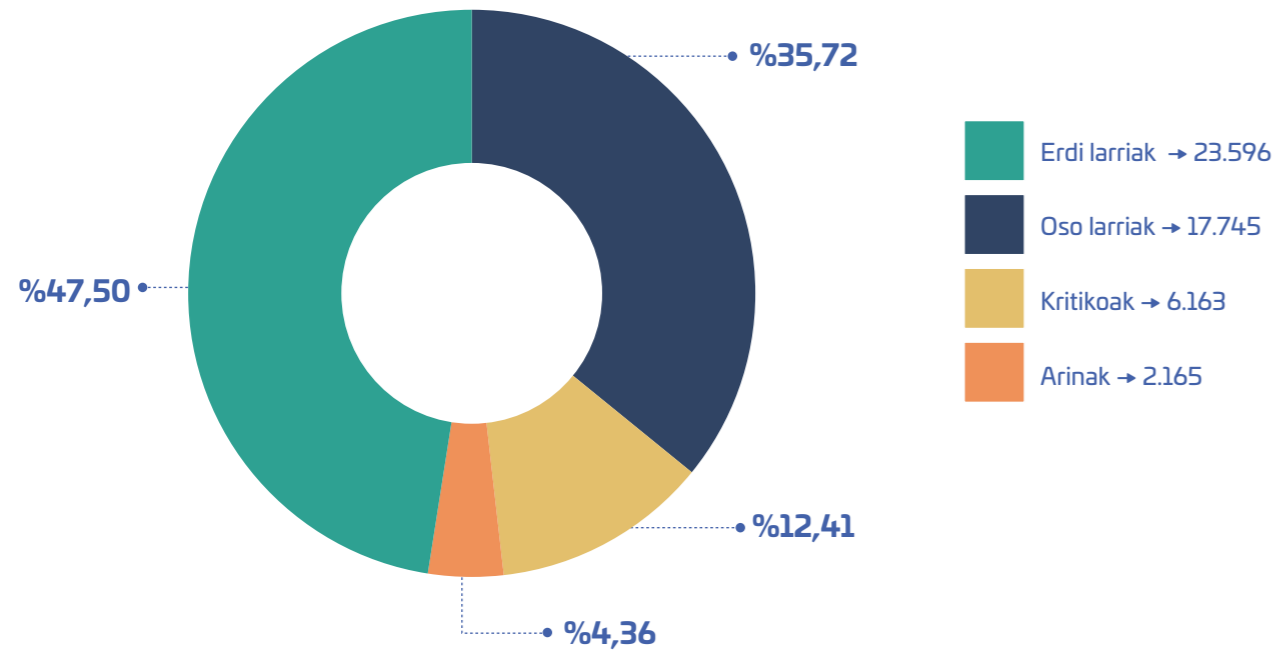
Aipatutako aldiaren zehar bereziki garrantzitsuak izan diren kalteberatasunak nabarmentzen dira

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 minimizatzen.

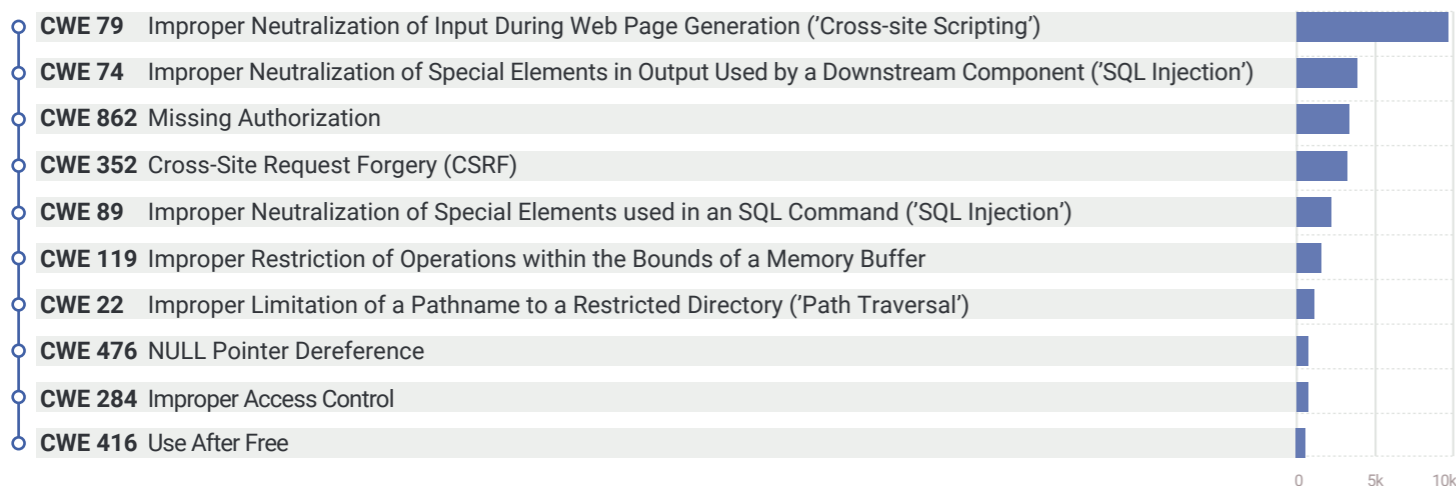
Datu nagusiak



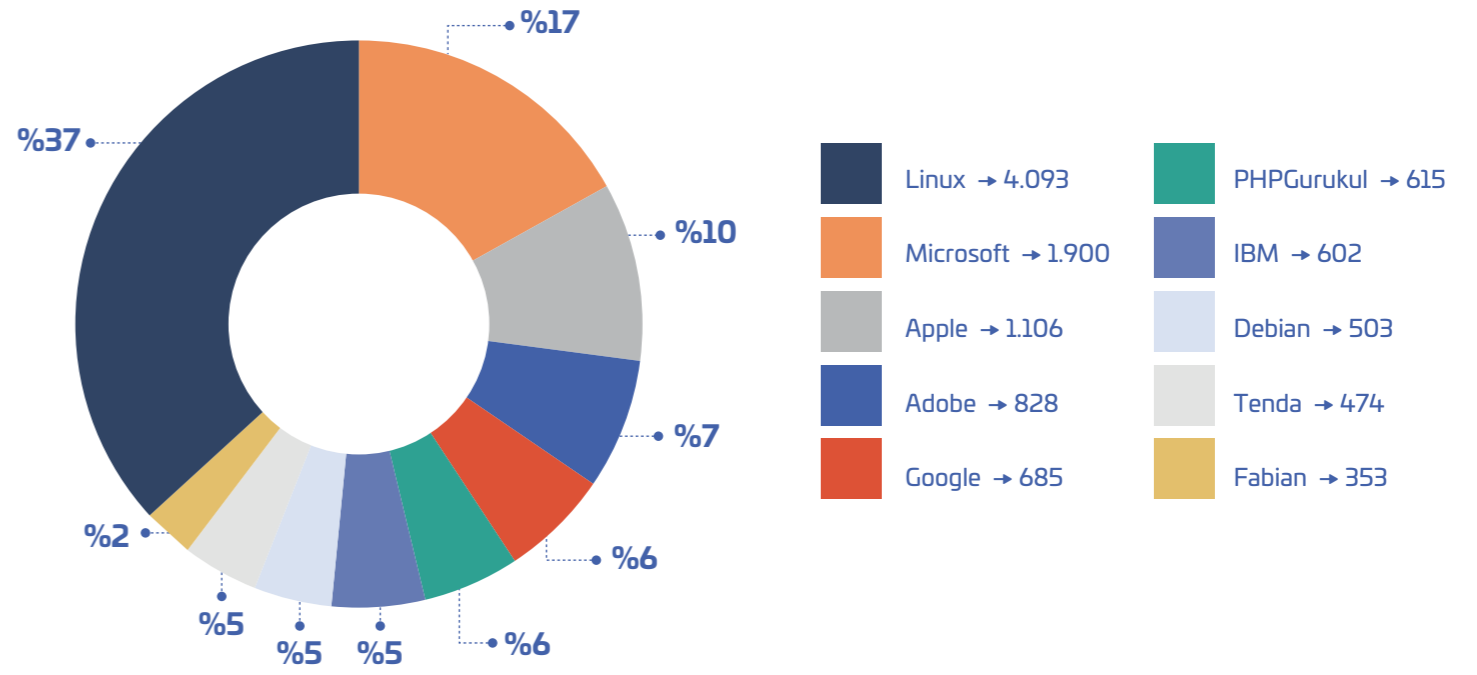
Larritasunaren arabera, ahultasunen sailkapena:



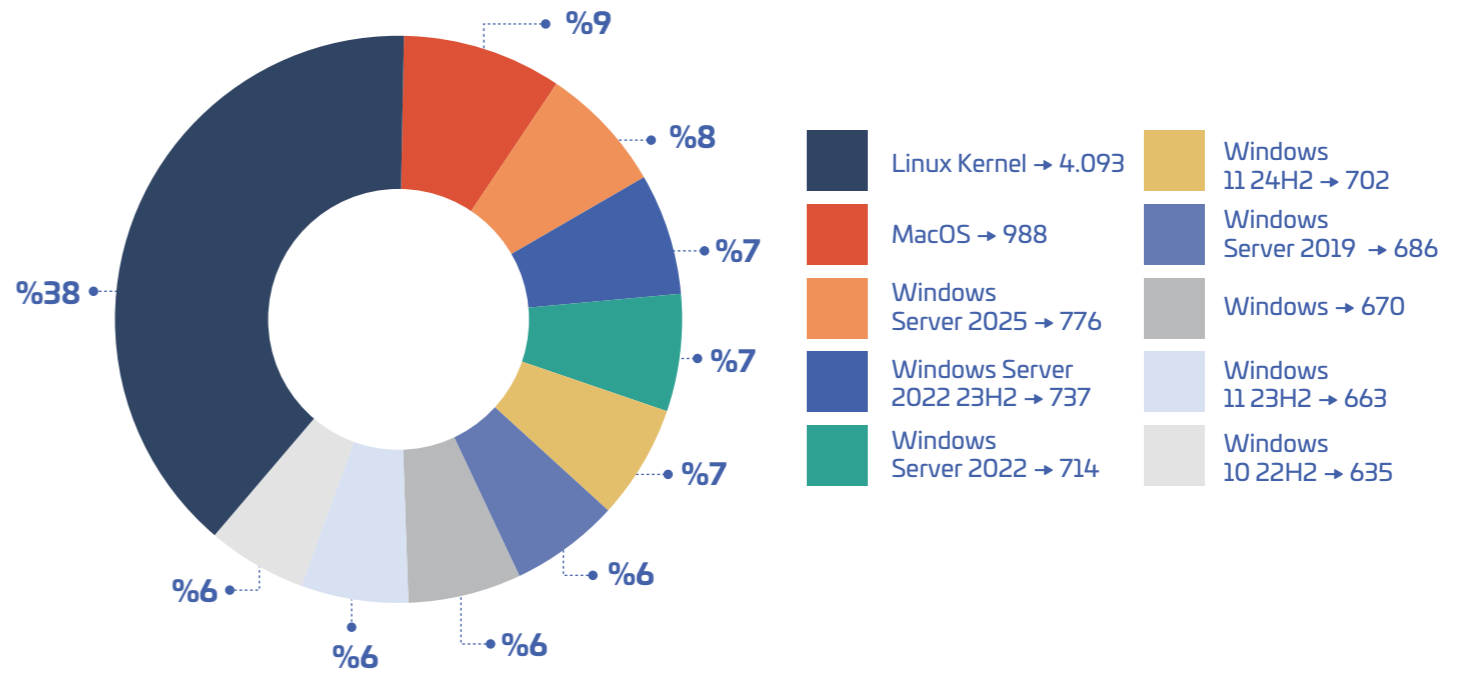
Top 10 CWE (Common Weakness Enumeration)



Identifikatutako ahuleziak dituzten punta-puntako 10 fabrikatzaile



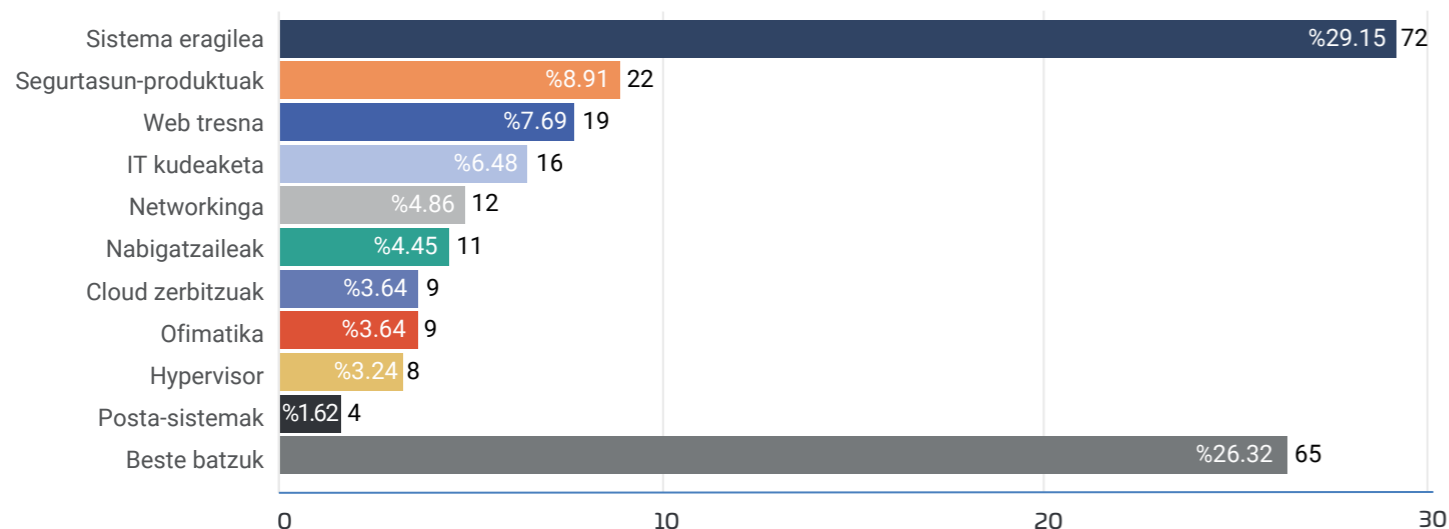
Ahulguneak dauzkaten 10 produktu punta-puntako



Aktiboki ustiatutako ahultasunak



Puntako 10 ahuleziak, softwarearen arabera



Benetan erabili diren ahulguneak dauzkaten puntako 5 fabrikatzaile/produktu

FABRIKATZAILEA	PRODUKTUAK	KANTITATEA
Microsoft	Windows SharePoint Internet Explorer .Net Framework Office	36
Apple	Multiple Products iOS and iPadOS iOS, iPadOS and macOS	9
Fortinet	FortiWeb Multiple Products FortiOs and FortiProxy FortiOs	8
Google	Chromium V8 Chromium Chromium Mojo	8
Cisco	Identity Services Engine Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Multiple Products iOS and iOS XE Small Business RV Series Routers	7

Ransomware-familek erabilitako puntu zaugarrietatik, urtean zehar zein izan diren ekinenak

Qilin - 1.062 biktima <ul style="list-style-type: none"> CVE-2023-27532 (7.5 larri) – Veeam Backup & Replication 	Play - 391 biktima <ul style="list-style-type: none"> CVE-2020-12812 (9.8 kritiko) – Fortinet CVE-2024-57727 (9.8 kritiko) – SimpleHelp RMM CVE-2018-13379 (9.1 kritiko) – Fortinet CVE-2022-41040 (8.8 larri) – Microsoft CVE-2022-41082 (8.0 larri) – Microsoft CVE-2025-29824 (7.8 larri) – Microsoft Windows CLFS 	Lynx - 275 biktima <ul style="list-style-type: none"> Ustez behintzat CVE gabe
Akira - 757 biktima <ul style="list-style-type: none"> CVE-2023-20269 (9.1 kritiko) – Cisco CVE-2020-3259 (7.5 larri) – Cisco CVE-2023-27532 (7.5 larri) – Veeam Backup & Replication 	InCRansom - 389 biktima <ul style="list-style-type: none"> CVE-2023-3519 (9.8 kritiko) – Citrix 	DragonForce - 228 biktima <ul style="list-style-type: none"> Ustez behintzat CVE gabe
Clop - 523 biktima <ul style="list-style-type: none"> CVE-2024-50623 (9.8 kritiko) – Cleo CVE-2023-0669 (9.3 kritiko) – GoAnywhere MFT CVE-2023-34362 (9.1 kritiko) – MOVEit Transfer CVE-2024-55956 (9.1 kritiko) – Cleo CVE-2021-27101/27102/27103/27104 (9.1 kritiko) – Accellion FTA 	Safepay -377 biktima <ul style="list-style-type: none"> Ustez behintzat CVE gabe 	Babuk - 219 biktima <ul style="list-style-type: none"> CVE-2021-21974 (9.8 kritiko) – VMware ESXi CVE-2021-27876/27877/27878 (9.8 kritiko) – Veritas Backup Exec
		DevMan - 196 biktima <ul style="list-style-type: none"> Ustez behintzat CVE gabe

Ondorioak

Hazkunde iraunkorra eta mehatxuen larritasunaren hazkunde kualitatiboa:

- Aurreko urtearekin alderatuta, argitaratutako ahulezien hazkundeak % 22,34an jarraitzen du, eta aktiboki ustiatutakoek % 31,38 egin zuten gora -> exploitak garatzeko ahalmen handiagoa eta ustiapen-abiadura handiagoa.
- Ahultasun kritikoak eta altuak ia bikoiztu egin dira, % 24,45etik % 48,13ra.

Ransomwarearen bilakaera:

- Qilin da lider berria**, Akirak eta Clopek jarraituta.
- Ustiatzen diren CVEetan, dibertsifikazioa mantentzen da: fitxategien transferentziarako produktuak, backup-ak eta konektibitate-azpiegitura berreskuratzea.
- Taldeek CVE-2024 eta CVE-2025 ahultasunak dituzte, eta CVE historiko frogatuen erabilerari eusten diote, hala nola Zerologon eta Fortineten ahultasunak.
- CVE ezagunak ustiatu gabe aritzen diren SafePay, Lynx, DragonForce eta DevMan talde berrien sendotzea.

Fabrikatzaileen eta eraso-bektoreen hazkunde adierazgarriak:

- Linux, Microsoft eta Apple dira igogaren buru, eta Linux Kernelek %38ari eutsi dio.
- Sistema eragileek modu aktiboan ustiatutako ahultasunen % 29,15 osatzen dute, eta % 89ko hazkundera izan dute.

➔ Gero eta sofistikuagoak dira eraso-teknikak, ekosistema kriminalaren dibertsifikazioa eta babes-estrategia moldagarriak behar dituzten exploit zabalagoen armategiak, adabaki bizkorak eta threat intelligence testuinguruan oinarritutako arrisku-kudeaketa.