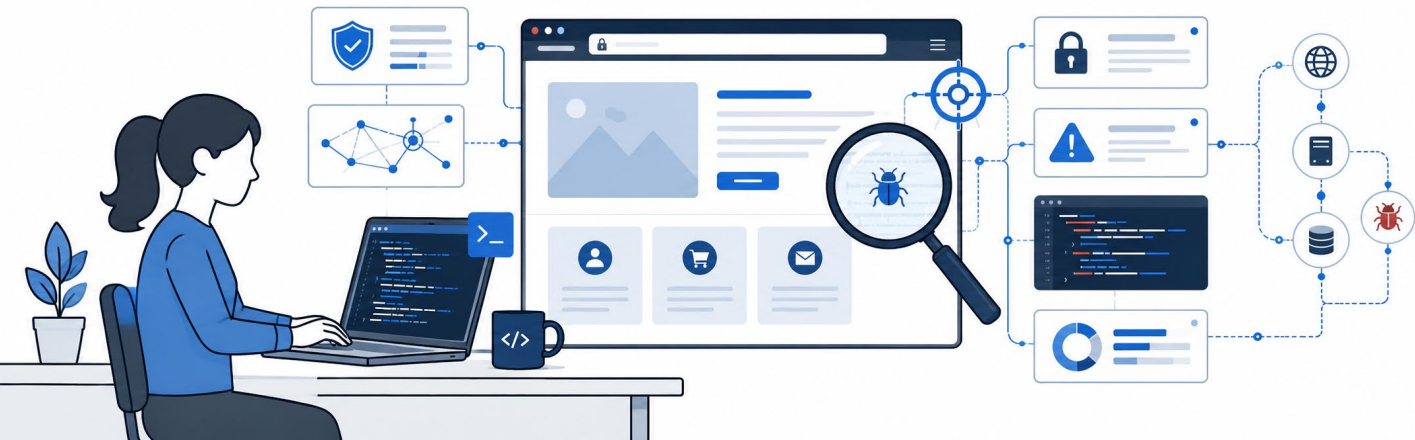


2026ko lehen seihipilekoan identifikatutako kalteberatasunak



Jarraian, 2026ko lehen seihipilekoan identifikatutako kalteberatasunen datu kuantitatiboak eta kualitatiboak adierazten dira, egungo egoera eta urte honetarako joera ebaluatu ahal izateko. Txostenean, aipatutako aldian garrantzi berezia izan duten kalteberatasunak nabarmentzen dira.

Aktiboki ustiatzen ari direnak eta biktima gehien dituzten ransomware familiekin lotuta daudenak sartzen dira. Aurkikuntza horiek nabarmentzen dute eguneratze-politikak eta kalteberatasunak kudeatzeko politikak ezartzearen garrantzia, horiek ustiatzearen ondorioz kaltetua izateko arriskua minimizatzeko helburuarekin.



35.494

Argitaratutako kalteberatasunak
▲ +61,70% vs S1 2025 (21.950→35.494)

2.538

Kaltetutako fabrikatzaileak
▲ +107,01% vs S1 2025 (1.226→2.538)

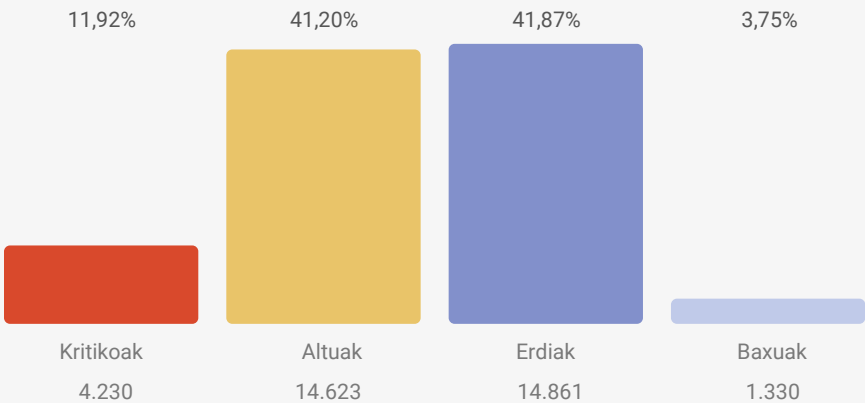
1.639

Aktiboki ustiatuak (guztira)
▲ +18,68% vs S1 2025 (1.381→1.639)

146

Ustiapen aktiboan berriak
▲ +9,77% vs S1 2025 (133→146)

Banaketa larritasunaren arabera



* 450 kalteberatasunek ez dute larritasunik esleitura (CVSS faltan)

10 fabrikatzaile nagusiak

Identifikatutako kalteberatasun kopuruaren arabera

1	Linux	3.082	33%
2	Microsoft	1.681	18%
3	Google	1.291	14%
4	Apple	1.213	13%
5	Openclaw	447	5%
6	Oracle	441	5%
7	IBM	300	3%
8	Apache	296	3%
9	Adobe	275	3%
10	Tenda	258	3%

10 produktu nagusiak

Identifikatutako kalteberatasun kopuruaren arabera

1	Linux Kernel	3.082	36%
2	MacOS	1.147	14%
3	Windows	1.053	12%
4	Chrome	1.008	12%
5	Openclaw	447	5%
6	Android	396	5%
7	Windows Server 2025	342	4%
8	Windows 11 24H2	332	4%
9	Windows 11 25H2	331	4%
10	Windows Server 2022 23H2	323	4%

Aktiboki ustiatutako kalteberatasunak

1.639

Metatutako kalteberatasun ustiatuak, guztira
▲ +18,68% metatutako guztizkoaren hazkundera vs S1 2025 (1.381→1.639)

146

S1 2026-en dauden kalteberatasun berriak ustiapen aktiboan
▲ +9,77% ustiatu berrien hazkundera vs S1 2025 (133→146)

10 kalteberatasun nagusiak eragindako softwarearen arabera

Aktiboki ustiatutako kalteberatasunen banaketa kategoriaren arabera

Sistema eragile	21	21,64%
IT Kudeaketa	15	15,46%
Networking	8	8,24%
Segurtasun produktuak	8	8,24%
Ofimatika	7	7,21%
Posta-sistemak	6	6,18%
Cloud zerbitzuak	6	6,18%
Bilatzaileak	5	5,15%
Azpiegitura	5	5,15%
Web tresnak	3	3,09%
Besteak	13	13,40%

Aktiboki ustiatutako kalteberatasunak dituzten 5 fabrikatzaile-produktu nagusiak

FABRIKATZAILEA	PRODUKTUAK	KOPURUA
Microsoft	Windows (11), Office (4), Defender (3), Internet Explorer (2), Configuration Manager (1)	21
Cisco	Catalyst SD-WAN Manager (4), Unified Communications Manager (2), Catalyst SD-WAN (1), Catalyst SD-WAN Controller (1)	8
Apple	Multiple Products (6), iOS and iPadOS (1)	7
Google	Chromium V8 (2), Chromium (1), Dawn (1), Skia (1)	5
Ivanti	Endpoint Manager Mobile EPMM (3), Endpoint Manager EPM (1), Sentry (1)	5

2026ko lehen sei hilekoan aktiboen egon diren ransomware familiek ustiatutako kalteberetasunak



Qilin 1.121 biktima 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy 9.6 CVE-2024-21762 Fortinet FortiOS 9.3 CVE-2026-50751 Check Point VPN 9.3 CVE-2025-5777 Citrix NetScaler ADC/GW 8.8 CVE-2024-1708 ConnectWise ScreenConnect 7.5 CVE-2023-27532 Veeam Backup & Replication	Thegentlemen 710 biktima BERRIA 10.0 CVE-2026-20131 Cisco Secure Firewall FMC (RCE) 10.0 CVE-2025-32433 Erlang/OTP SSH 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy 9.3 CVE-2026-50751 Check Point Security GW 8.8 CVE-2025-33073 Windows SMB/Kerberos Relay	Akira 533 biktima +43% 9.3 CVE-2024-40766 SonicWall SonicOS SSL VPN 9.1 CVE-2023-20269 Cisco ASA 7.5 CVE-2020-3259 Cisco AnyConnect 7.5 CVE-2023-27532 Veeam Backup & Replication	Dragonforce 425 biktima BERRIA 9.8 CVE-2024-57726/27/28 SimpleHelp RMM 9.3 CVE-2025-5777 Citrix NetScaler (CitrixBleed 2) 8.2 CVE-2023-46805 Ivanti Connect Secure 5.5 CVE-2025-61155 Tower of Fantasy driver (BYOVD)	Incransom 425 biktima +217% 9.8 CVE-2023-3519 Citrix NetScaler ADC/Gateway
NightSpire 351 biktima BERRIA 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy	Lockbit5 326 biktima BERRIA 9.8 CVE-2023-27350 PaperCut MF/NG 9.8 CVE-2024-55591 Fortinet FortiOS/FortiProxy 9.3 CVE-2023-0669 Fortra GoAnywhere MFT	Play 288 biktima +36% 9.8 CVE-2020-12812 Fortinet SSL VPN 9.8 CVE-2024-57727 SimpleHelp RMM 9.1 CVE-2018-13379 Fortinet FortiOS 8.8 CVE-2022-41040 Microsoft Exchange 8.8 CVE-2022-41080 Microsoft Exchange 8.0 CVE-2022-41082 Microsoft Exchange RCE 7.8 CVE-2025-29824 Microsoft Windows CLFS	Clop 256 biktima -37% 9.8 CVE-2024-50623 Cleo (carga/descarga) 9.3 CVE-2023-0669 GoAnywhere MFT 9.1 CVE-2023-34362 MOVEit Transfer SQL injection 9.1 CVE-2024-55956 Cleo RCE 9.1 CVE-2021-27101/02/03/04 Accellion FTA	CoinBase Cartel 224 biktima BERRIA Publikoki esleitutako CVErik gabe

CVE-2024-55591 (FortiOS/FortiProxy · CVSS 9.8 kritikoa)

Seihilekoko kalteberatasunik partekatuen: gutxienez 10 talde aktiboenetako 4tan dago (Qilin, Thegentlemen, NightSpire eta Lockbit5). CISA KEV katalogoan sartuta dago.

Ondorioak

- 1

Hazkunde esponentziala: joera moderatuaren haustura.

Argitaratutako kalteberatasunak 35.494ra iritsi dira (+61,70% vs S1 2025), aurreko urteko hazkunde moderatua (+5,05%) hautsiz. Eragindako fabrikatzaileak bikoitza baino gehiago dira: 2.538 vs 1.226 2025en.
- 2

Kritikotasunaren larriagotze gogorra.

Kritikoak + Altuak % 18,11tik % 53,12ra igaro dira —guztizkoaren erdia baino gehiago—. Kritikoak ia bikoiztu egin dira (% 6,58→% 11,92) eta altuak ia laukoiztu egin dira (% 11,53→% 41,20).
- 3

Linux, Microsoft eta Google dira hazkundearen buru.

Linux Kernel: 876→3.082 (+% 252). Microsoft: 377→1.681 (+% 346). Googlek 1.291 kalteberatasunekin egin du agerpena, 2025ean ia hondarrezko presentzia izan ondoren (109).
- 4

Ustiapen aktiboa: hazkunde jasankorra.

Ustiapen aktiboa duten kalteberatasunak 1.639ra iritsi dira guztizkoan (+18,68% vs 1.381 S1 2025en); 146 inkorporazio berri izan dira (+9,77% vs 133). Sistema eragileek biltzen dute 21,64%, eta ondoren IT kudeaketak (15,46%). Microsoft da buru ustiatutako 21 kalteberatasunekin, eta ondoren datoz Cisco (8), Apple (7), Google (5) eta Ivanti (5).
- 5

Perimetroa bektore kritiko gisa ransomwarean.

Ransomware taldeek ustiatutako CVEak konektagarritasunean (Fortinet, Cisco, Citrix, Check Point), babeskopietan (Veeam) eta fitxategi-transferentzian zein RMMetan (GoAnywhere, MOVEit, Cleo, SimpleHelp) biltzen dira.
- 6

Eredu bikoitza ransomware taldeen armategietan.

Berrerabilera historikoa: CVE-2018-13379, CVE-2020-3259 eta CVE-2021-27101/104 aktibo daude oraindik 2026an. Time-to-exploit-aren azelerazioa: CVE-2025-32433 eta CVE-2026-20131 argitaratu diren sei hileko berean agertu dira.

Gomendioak

- Benetako arriskuaren araberako adabakitze lehenetsia

Lehentasuna baieztatutako ustiapen aktiboan oinarritzea (CISA KEV), eta ez CVSS hutsean. Gehieneko epea 48-72 ordukoa da perimetroko kalteberatasun kritikoetarako.
- Perimetroaren esposizioaren murrizketa

Internetetik eskuragarri dauden VPNak, firewallak, RMMak, fitxategiak transferitzeko plataformak eta babeskopiak ikuskatzea.
- Monitorizazio indartua

Linuxek (+% 252), Microsoftek (+% 346) eta Googlek (+% 1.084) argitaratutako kalteberatasunen hazkundera gidatzen dute. Hardening-a aplikatu berehalako adabakitzea bideragarria ez den kasuetan.
- Testuinguruan jarritako mehatxu-inteligentzia

kalteberatasunak ransomware taldeen jarduerarekin erlazionatzea, bektoreei aurrea hartzeko ustiapen masiboa gertatu baino lehen.
- Prestakuntza eta kontzientziazioa

Ofimatikako eta postako gorakadak etengabeko prestakuntzaren beharra indartzen du, adabakitze teknikoaren osagarri gisa.
- Erantzun-plan azeleratuak

Time-to-exploit-a orduetara laburtu da. Erantzun-planek argitaratzen denetik 24 ordu baino lehenagoko konpromisoak aurreikusi behar dituzte.

Aurreikuspenak

- Aurrekorik gabeko bolumena

kalteberatasunak aurkitzeko aplikatutako adimen artifizialaren ondorioz, urteko guztizkoak lehen aldiz 70.000 kalteberatasunen muga gaindituko duela aurreikusten da.
- Larritasun jasankorra

Kritikoen eta altuen proportzioa % 50etik gora mantenduko da, larritasun-estandar berria finkatuz.
- Linux eta cloud ardatz bezala

Linux Kernelak eta cloud inguruneek kalteberatasunen foku nagusiak izaten jarraituko dute bolumenari dagokionez.
- Perimetroaren ustiapena

Ransomware taldeek CVEak ustiatzen jarraituko dute Fortinet, Cisco eta Citrix-en argitaratu eta lehen orduetan, bereziki konektagarritasun-gailuei eragiten dietenean.