



ESCUELA
POLITÉCNICA
NACIONAL

ESCUELA POLITÉCNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS



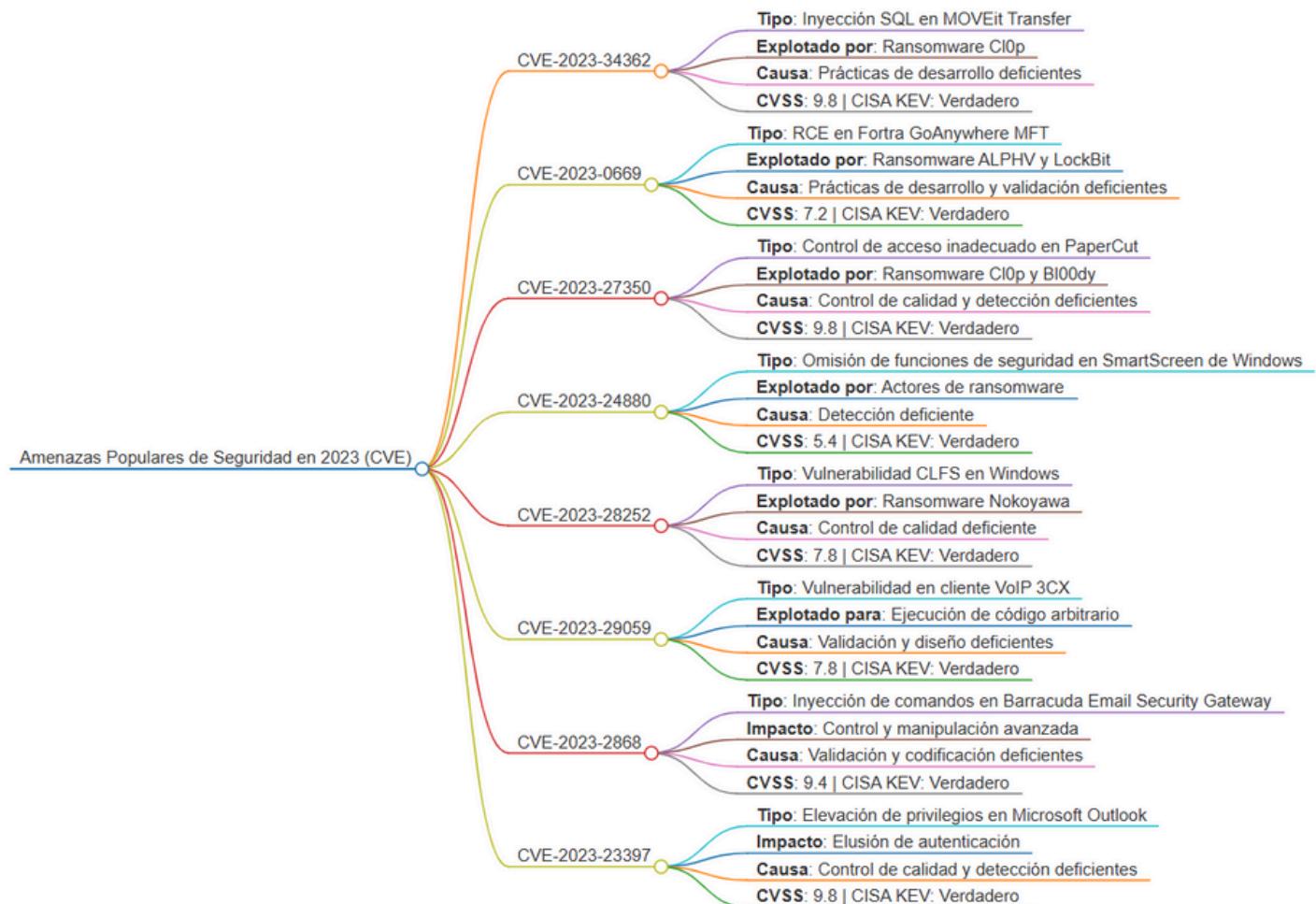
2024 Vulnerability Statistics Report

Grupo #2
Integrantes:
Esteban Hidalgo
Johan Baño
Luis Rocha
Nicolas Reinoso

Profesor: Ing. Juan Herrera
Fecha: 26/10/2024

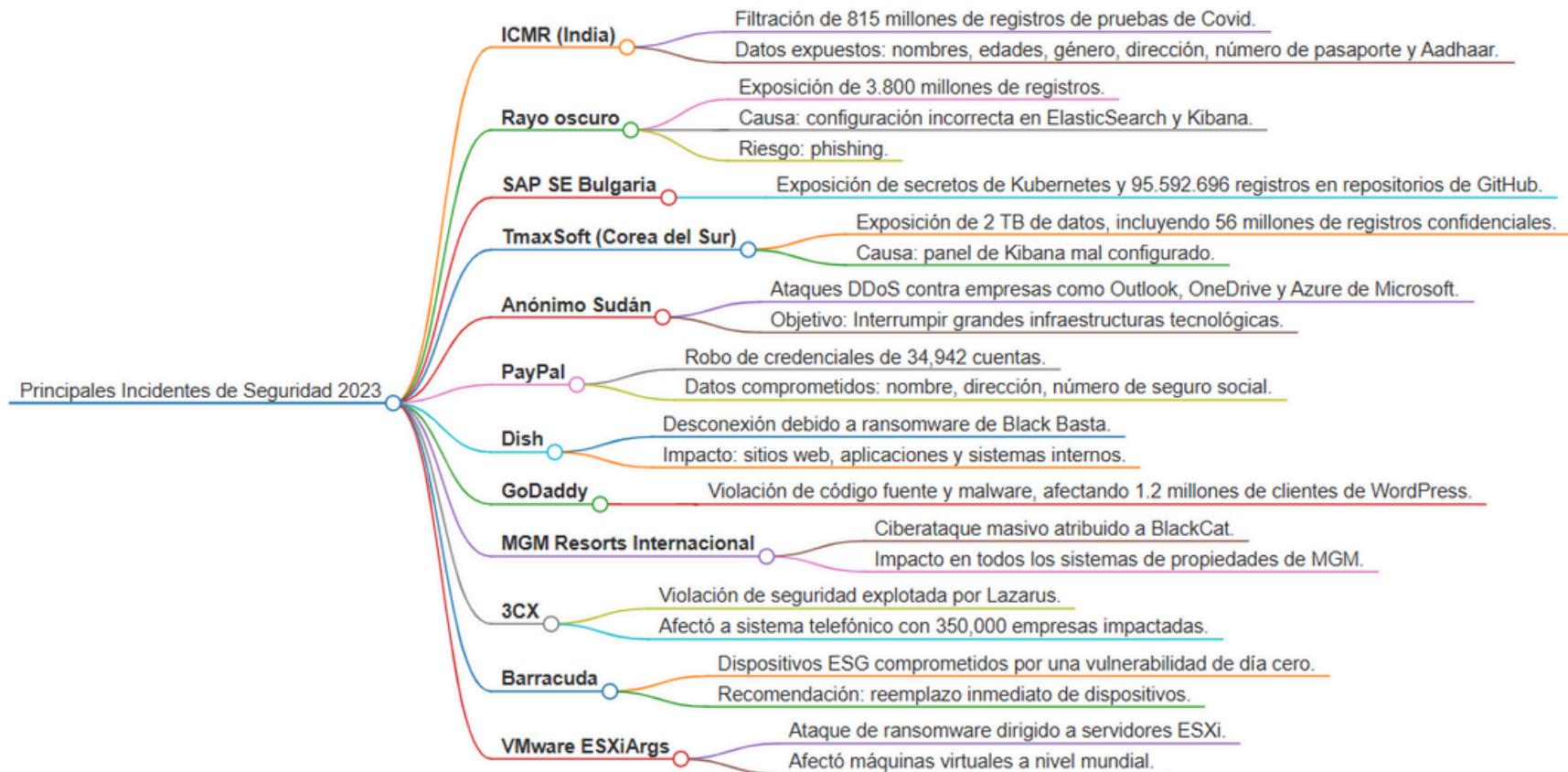
VULNERABILIDADES A TENER EN CUENTA EN 2023

El siguiente mapa mental muestra algunos de los CVE populares aprovechados por los actores de amenazas en 2023

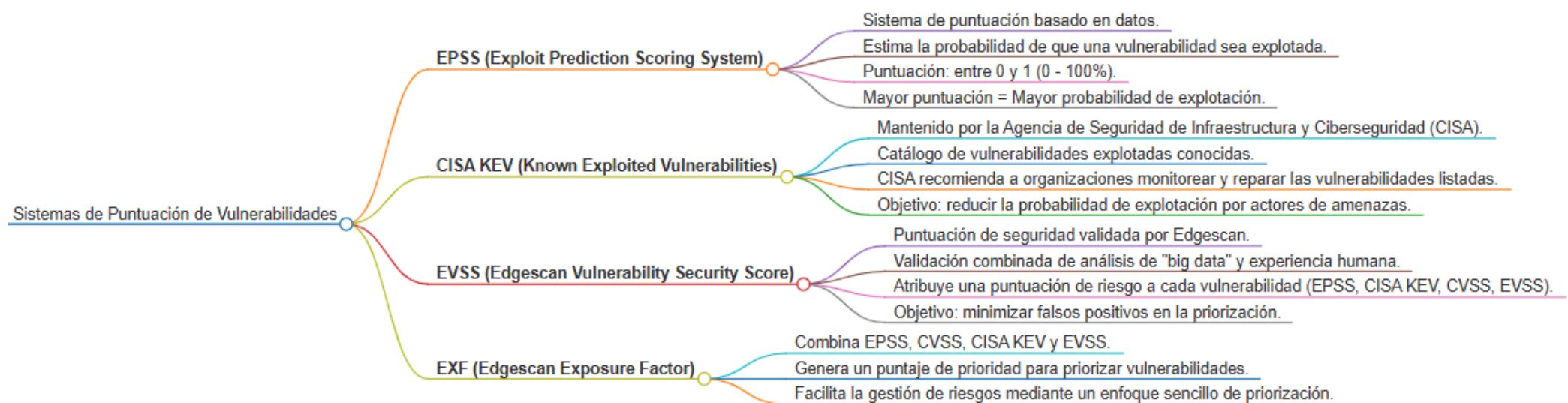


LOS INCUMPLIMIENTOS MÁS IMPORTANTES EN 2023

El siguiente mapa mental muestra varias infracciones ciberneticas importantes que afectaron a millones de personas



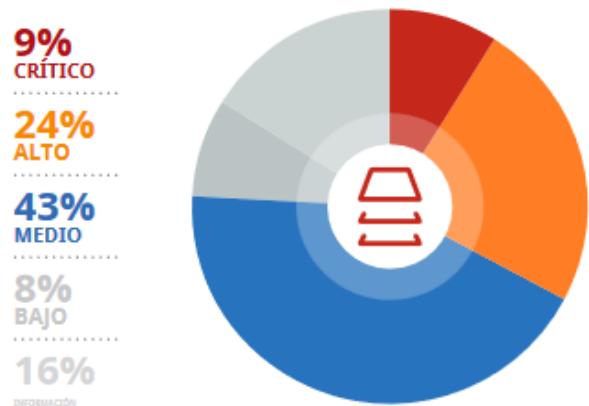
Gravedad de la vulnerabilidad EPSS, CISA KEV y EVSS



DENSIDAD DE RIESGO

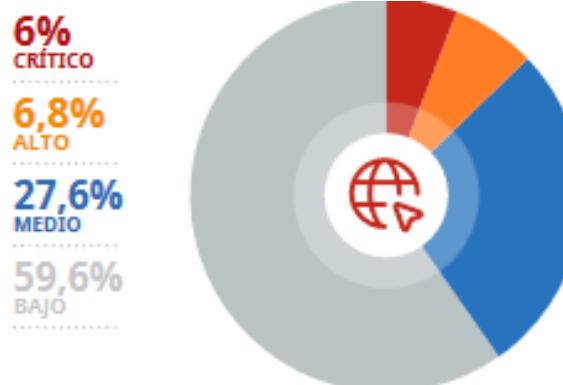
Desglose de vulnerabilidades por gravedad, descubiertas en aplicaciones web, API e implementaciones de red/host

Dispersión de la gravedad en toda la pila (red, web y API combinadas)



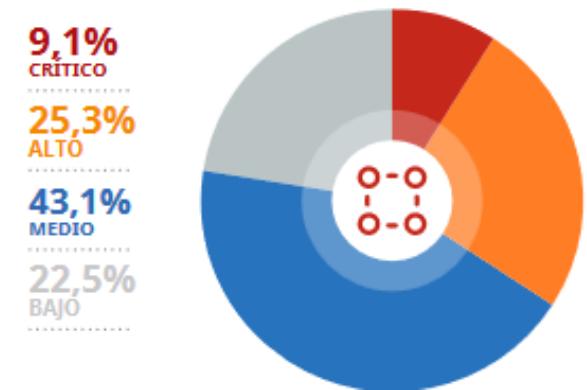
Gravedad basada en Edgescan EVSS

Dispersión de vulnerabilidades de API y aplicaciones web por gravedad



Vulnerabilidades como inyección SQL, se descubren fácilmente (19.47%)

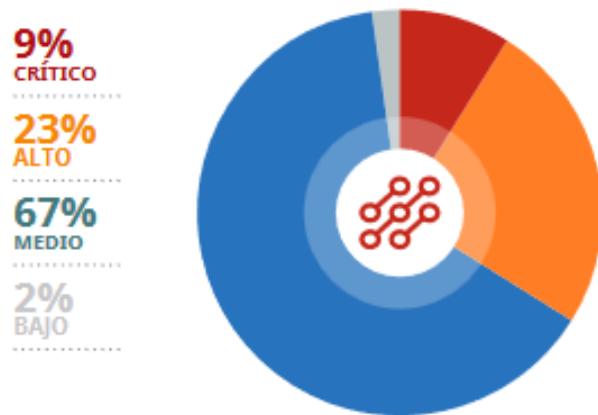
Dispersión de vulnerabilidades de red/host por gravedad



Gravedad basada en Edgescan EPSS

FALLAS DE PCI POR GRAVEDAD

Fallas de PCI por gravedad



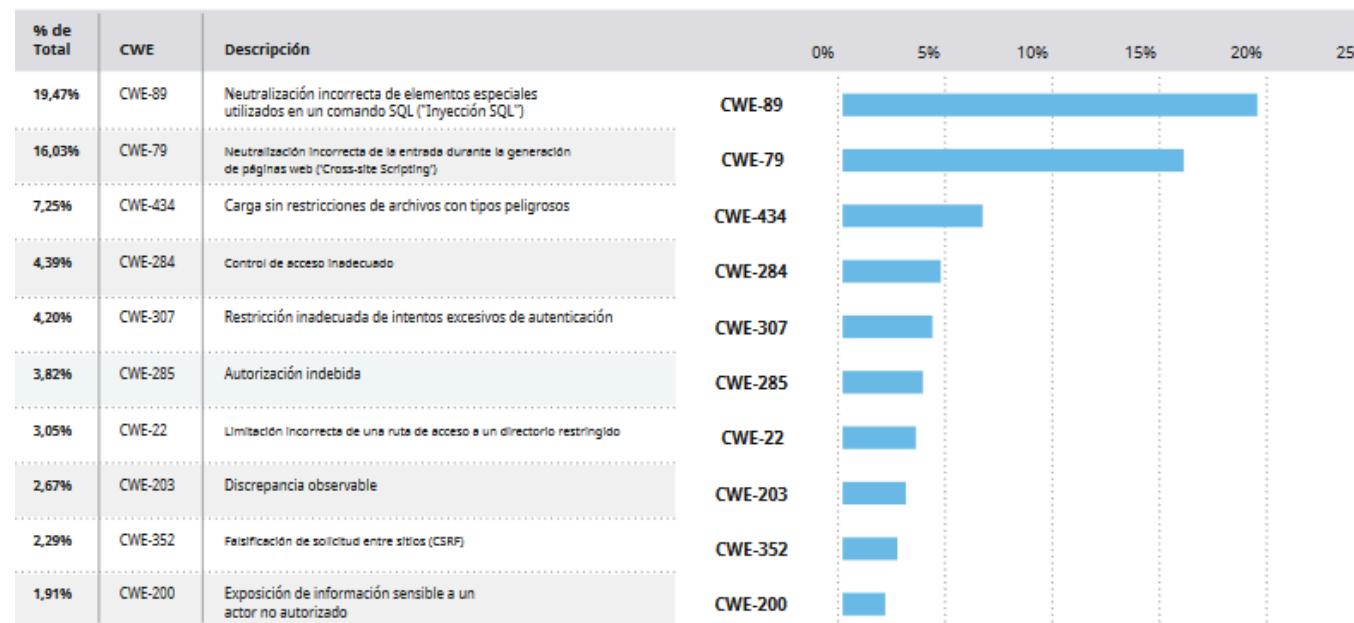
Muchas fallas de PCI son de bajo riesgo de ser explotadas por su bajo puntaje en EPSS

EPSS más alto	CVE
97%	CVE-2020-1938
97%	CVE-2014-0224
60%	CVE-2023-42795, CVE-2023-44487, CVE-2023-45648
98%	CVE-2014-3566

ERRORES DE GRAVEDAD ALTA Y CRÍTICA MÁS COMUNES SEGÚN CWE: APLICACIONES WEB

CWE es una lista de tipos de debilidades de software y hardware desarrollada por la comunidad

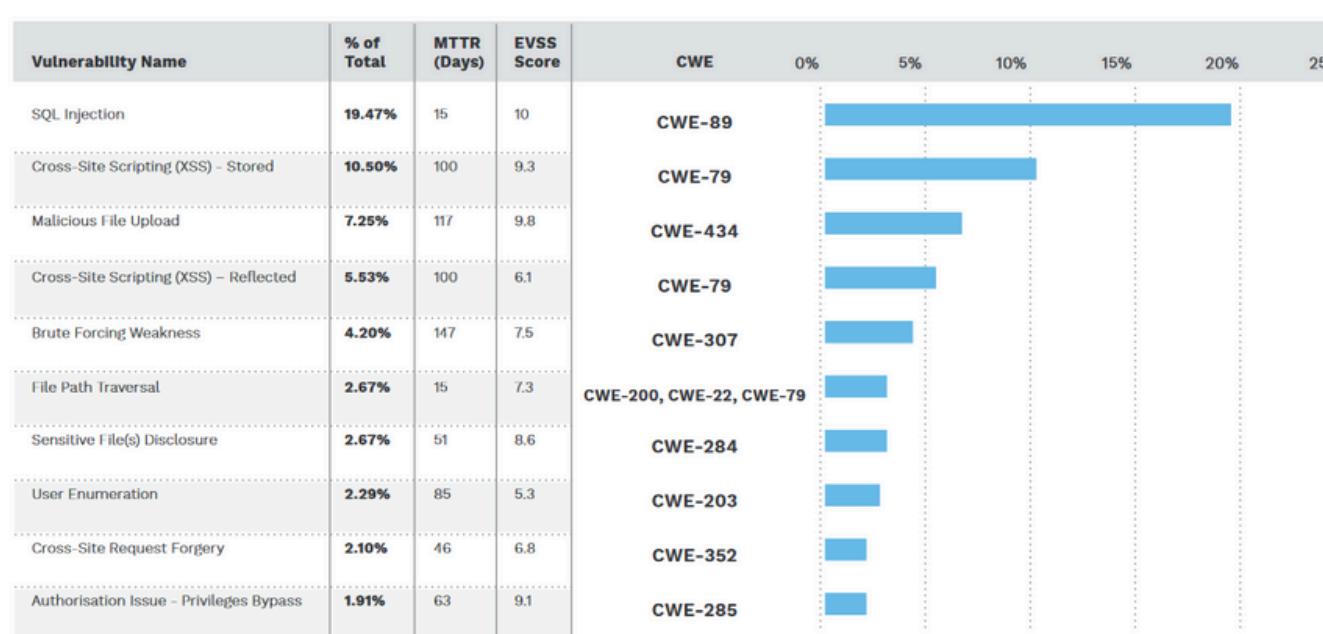
Dispersión de CWE: gravedad alta y crítica





Vulnerabilidades más comunes de gravedad alta y crítica en aplicaciones web

Web Application Vulnerabilities



La vulnerabilidad crítica más común en aplicaciones web es la inyección SQL (CWE-89), una vulnerabilidad que data de 1998.



CISA KEV

A partir de enero de 2024, a continuación se muestra la lista de vulnerabilidades asociadas con cada proveedor según CISA KEV.

Microsoft 278	Apple 73	CISCO 69	Adobe 67	Google 54
Oracle 33	Apache 31	Vmware 19	Citrix 16	D-Link 16
Ivanti 16	Atlassian 12	Fortinet 12	Linux 12	Mozilla 11
Samsung 11	QNAP 11	SAP 10	Trend Micro 10	SonicWall 9

DISPERSIÓN DE VULNERABILIDADES DE CISA KEV POR PROVEEDOR



Vulnerabilidad más común con EPSS >0,8

80% PROBABILITY OF BREACH – PUBLIC INTERNET FACING

MTTR (tiempo medio de reparación) es la velocidad con la que reparamos las vulnerabilidades descubiertas. Desde el descubrimiento hasta la reparación y la validación de la reparación

CISA KEV muestra si la vulnerabilidad está incluida en el catálogo de exploits conocidos administrado por la Agencia de Infraestructura y Seguridad Cibernética (CISA)

EPSS es la probabilidad de explotación según los datos de first.org.

"Existe código de explotación"
significa si
el código de explotación está
disponible libremente
en Internet público.



Vulnerabilidad más común con EPSS >0,8

80% PROBABILITY OF BREACH – NON-PUBLIC INTERNET FACING

Technology	% of Total	MTTR (Days)	CWE	CVE	CISA KEV	CVSS	EPSS	EXF	Exploit Code Exists
SSL/TLS: Weak Cipher Suites	40.30%	34.7	CWE-310, CWE-326, CWE-327	CVE-2013-2566, CVE-2015-2808, CVE-2015-4000	FALSE	5.9	0.97493	83	
SSL/TLS Difflie-Hellman Modulus < 1024 Bits (l. op.jam)	22.00%	50.5	CWE-310	CVE-2015-4000	FALSE	3.7	0.97493	82	
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	12.05%	48.2	CWE-310	CVE-2014-3566	FALSE	3.4	0.97505	82	Yes
SUSE: Security Advisory Multiple Vulnerabilities	7.40%	49.3	CWE-119, CWE-120, CWE-121, CWE-122, CWE-125, CWE-126, CWE-128, CWE-190, CWE-20, CWE-416, CWE-457, CWE-476, CWE-668, CWE-674, CWE-787, CWE-823	CVE-2009-0316, CVE-2016-1248, CVE-2017-17087, CVE-2017-5953, CVE-2017-6349, CVE-2017-6350, CVE-2021-3778, CVE-2021-3786, CVE-2021-3872, CVE-2021-3876, CVE-2021-3903, CVE-2021-3927, CVE-2021-3928, CVE-2021-3968, CVE-2021-3973, CVE-2021-3974, CVE-2021-3975, CVE-2021-3976, CVE-2021-3977, CVE-2021-3978, CVE-2021-4106, CVE-2021-4102, CVE-2021-4103, CVE-2021-46058, CVE-2022-0108, CVE-2022-0235, CVE-2022-0261, CVE-2022-0318, CVE-2022-0319, CVE-2022-0324, CVE-2022-0394, CVE-2022-0361, CVE-2022-0392, CVE-2022-0404, CVE-2022-0413, CVE-2022-0696, CVE-2022-1381, CVE-2022-1420, CVE-2022-1616, CVE-2022-1619, CVE-2022-1620, CVE-2022-1720, CVE-2022-1733, CVE-2022-1735, CVE-2022-1771, CVE-2022-1785, CVE-2022-1796, CVE-2022-1814, CVE-2022-1884, CVE-2022-1888, CVE-2022-1921, CVE-2022-1968, CVE-2022-2124, CVE-2022-2126, CVE-2022-2128, CVE-2022-2129, CVE-2022-2175, CVE-2022-2182, CVE-2022-2183, CVE-2022-2206, CVE-2022-2207, CVE-2022-2208, CVE-2022-2210, CVE-2022-2231, CVE-2022-2297, CVE-2022-2264, CVE-2022-2284, CVE-2022-2298, CVE-2022-2298, CVE-2022-2298, CVE-2022-2304, CVE-2022-2343, CVE-2022-2344, CVE-2022-2345, CVE-2022-2522, CVE-2022-2571, CVE-2022-2580, CVE-2022-2681, CVE-2022-2680, CVE-2022-2616, CVE-2022-2617, CVE-2022-2810, CVE-2022-2845, CVE-2022-2849, CVE-2022-2862, CVE-2022-2814, CVE-2022-2889, CVE-2022-2923, CVE-2022-3016, CVE-2022-3034, CVE-2022-3039, CVE-2022-3134, CVE-2022-3153, CVE-2022-3234, CVE-2022-3235, CVE-2022-3278, CVE-2022-3296, CVE-2022-3297, CVE-2022-3324, CVE-2022-3362, CVE-2022-3705	TRUE	9.8	0.96717	83	Yes
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	3.97%	71.6	CWE-310	CVE-2015-0204	FALSE	4.3	0.96454	82	
OpenSSL 'ChangeCipherSpec' MITM Vulnerability	2.95%	30.6	CWE-326	CVE-2014-0224	FALSE	7.4	0.97404	84	
Apache Tomcat - Multiple Vulnerabilities	2.35%	16.0	CWE-444, CWE-401, CWE-476, CWE-835, CWE-502, CWE-269, CWE-78, CWE-601, CWE-200, CWE-287, CWE-94, CWE-19, CWE-20	CVE-2020-9484, CVE-2020-1936, CVE-2020-1938 , CVE-2018-11784, CVE-2012-0874, CVE-2013-4810	FALSE	7	0.8836	83	Yes

MTTR (tiempo medio de reparación) es la velocidad con la que reparamos las vulnerabilidades descubiertas. Desde el descubrimiento hasta la reparación y la validación de la reparación

CISA KEV muestra si la vulnerabilidad está incluida en el catálogo de exploits conocidos administrado por la Agencia de Infraestructura y Seguridad Cibernética (CISA)

EPSS es la probabilidad de explotación según los datos de first.org.

"Existe código de explotación" significa si el código de explotación está disponible libremente en Internet público.



Vulnerabilidad más común con EPSS >0,8

80% PROBABILITY OF BREACH – NON-PUBLIC INTERNET FACING

MTTR (tiempo medio de reparación) es la velocidad con la que reparamos las vulnerabilidades descubiertas. Desde el descubrimiento hasta la reparación y la validación de la reparación

CISA KEV muestra si la vulnerabilidad está incluida en el catálogo de exploits conocidos administrado por la Agencia de Infraestructura y Seguridad Cibernética (CISA)

EPSS es la probabilidad de explotación según los datos de first.org.

"Existe código de explotación"
significa si
el código de explotación está
disponible libremente
en Internet público.



Gravedad alta y crítica más común (CVSS)

VULNERABILIDADES DE REDES QUE NO ESTÁN RELACIONADAS CON INTERNET

Technology	% of Total	MTTR (Days)	CWE	CVE	CISA KEV	CVSS	EPSS	Exploit Code Exists
SNMP Agent Default Community Names	7.57%	58.7	CWE-264	CVE-1999-0517	FALSE	7.5	0.45448	
Oracle Java SE Security Multiple Vulnerabilities - Windows	3.25%	44.1		CVE-2015-4734, CVE-2015-4803, CVE-2015-4805, CVE-2015-4806, CVE-2015-4835, CVE-2015-4842, CVE-2015-4843, CVE-2015-4844, CVE-2015-4860, CVE-2015-4872, CVE-2015-4881, CVE-2015-4882, CVE-2015-4883, CVE-2015-4893, CVE-2016-4902, CVE-2016-4903, CVE-2016-4911	TRUE	8.3	0.0833	Yes
Windows IExpress Untrusted Search Path Vulnerability	2.49%	48.9	CWE-426	CVE-2018-0598	FALSE	7.8	0.00846	
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	1.02%	49.5	CWE-200	CVE-2016-2183	FALSE	7.5	0.00547	
OpenSSL 'ChangeCipherSpec' MITM Vulnerability	1.01%	30.7	CWE-326	CVE-2014-0224	FALSE	7.4	0.97404	Yes
SUSE: Security Advisory Multiple Vulnerabilities	0.96%	51.3	CWE-125	CVE-2009-0316, CVE-2016-1248, CVE-2017-17087, CVE-2017-5953, CVE-2017-6349, CVE-2017-6350, CVE-2021-3778, CVE-2021-3796, CVE-2021-3872, CVE-2021-3875, CVE-2021-3903, CVE-2021-3927, CVE-2021-3928, CVE-2021-3968, CVE-2021-3973, CVE-2021-3974, CVE-2021-3984, CVE-2021-4019, CVE-2021-4068, CVE-2021-4136, CVE-2021-4166, CVE-2021-4192, CVE-2021-4193, CVE-2021-46058, CVE-2022-0128, CVE-2022-0213, CVE-2022-0261, CVE-2022-0318, CVE-2022-0319, CVE-20220351, CVE-2022-0359	FALSE	7.1	0.80025	



Gravedad alta y crítica más común (CVSS)

VULNERABILIDADES DE REDES QUE NO ESTÁN RELACIONADAS CON INTERNET

Microsoft Message Queuing (MSMQ) RCE Vulnerability (QueueJumper)	0.87%	20.6	CWE-20 CWE-787	CVE-2023-21554	FALSE	10	0.96122	Yes
VNC Brute Force Login	0.84%	15.9	CWE-287, CWE-307	-	FALSE	9	-	
OS End Of Life Detection	0.80%	45.8	CWE-1104, CWE-672	-	FALSE	10	-	
Xerox Printers Multiple Vulnerabilities - Ripple20 (XRX20.J) (XRX22-002)(No Creds) (RCE) (XRX20I/R20-05) (R20-05)	0.80%	55.8	CWE-125, CWE-190, CWE-191, CWE-20, CWE-200, CWE-415, CWE-787, CWE-862	CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2109, CVE-2016-2176, CVE-2018-17172, CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914	TRUE	10	0.04756	Yes



Gravedad alta y crítica más común (CVSS)

VULNERABILIDADES EXPUESTAS EN INTERNET PÚBLICO

Technology	% of Total	MTTR (Days)	CWE	CVE	CISA KEV	CVSS	EPSS	Exploit Code Exists
OpenBSD OpenSSH Multiple Vulnerabilities	34.1%	35.06	CWE-428	CVE-2023-38408, CVE-2023-28531	FALSE	9.8	0.04189	
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	18.9%	31.57	CWE-400	CVE-2002-20001	FALSE	7.5	0.00544	
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	11.8%	162.56	CWE-200	CVE-2016-2183	FALSE	7.5	0.00547	
PHP Multiple Vulnerabilities	7.1%	62.92	CWE-125	CVE-2016-9935, CVE-2017-16642, CVE-2018-7584, CVE-2017-7272, CVE-2018-10546, CVE-2018-10547, CVE-2018-10548, CVE-2018-10549, CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024, CVE-2019-9637, CVE-2019-9638, CVE-2019-9639, CVE-2019-9640, CVE-2019-9641, CVE-2021-21703, CVE-2022-31631, CVE-2022-4900, CVE-2022-31630, CVE-2022-37454	FALSE	9.8	0.95128	
Apache HTTP Server Multiple Vulnerabilities	3.0%	41.90	CWE-476	CVE-2021-31618, CVE-2021-34798, CVE-2021-39275, CVE-2021-40438, CVE-2021-44790, CVE-2023-25690, CVE-2021-33193, CVE-2023-27522, CVE-2019-17567, CVE-2020-13938, CVE-2020-13950, CVE-2020-35452, CVE-2021-26690, CVE-2021-26691, CVE-2021-30641	TRUE	9.8	0.97178	Yes
OpenSSL Multiple Vulnerabilities	2.6%	30.04	CWE-203, CWE-416, CWE-843	CVE-2014-0224, CVE-2021-3449, CVE-2021-3450, CVE-2021-3711, CVE-2021-3712, CVE-2022-4304, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-2650	FALSE	8.3	0.00127	



Gravedad alta y crítica más común (CVSS)

VULNERABILIDADES EXPUESTAS EN INTERNET PÚBLICO

Microsoft Exchange Server 2013 / 2016 / 2019 Multiple Vulnerabilities	2.2%	152.96		CVE-2021-41349, CVE-2021-42305, CVE-2021-42321, CVE-2022-41040, CVE-2022-41082, CVE-2022-23277, CVE-2022-24463, CVE-2023-21709, CVE-2023-35368, CVE-2023-35388, CVE-2023-36744, CVE-2023-36745, CVE-2023-36756, CVE-2023-36757, CVE-2023-36777, CVE-2023-38181, CVE-2023-38182, CVE-2023-38185	TRUE	8.8	0.90677	Yes
Rockwell Automation MicroLogix 1400 < 21.004 DoS Vulnerability	1.9%	41.90	CWE-306	CVE-2018-17924, CVE-2022-3166, CVE-2022-46670, CVE-2021-22658, CVE-2017-16740, CVE-2015-6486, CVE-2015-6488, CVE-2015-6490, CVE-2015-6491, CVE-2015-6492	FALSE	8.6	0.00056	Yes
Exim Internet Mailer, Multiple Vulnerabilities	1.6%	42.95	CWE-119, CWE-416, CWE-74, CWE-763	CVE-2023-42117, CVE-2023-42118, CVE-2023-42119, CVE-2022-37451, CVE-2021-38371, CVE-2022-3559, CVE-2022-3620	FALSE	7.79	0.00241	
ISC BIND Buffer Overflow Vulnerability	1.0%	74.86	CWE-120	CVE-2020-8625, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465, CVE-2018-5743, CVE-2021-25215, CVE-2022-38177, CVE-2022-38178, CVE-2023-2828, CVE-2023-3341	FALSE	8.1	0.21565	
Atlassian Jira Multiple Vulnerabilities	1.0%	84.89	CWE-287	CVE-2022-0540	FALSE	9.8	0.14417	



MTTR

El MTTR es un KPI de mantenimiento, cuyas siglas provienen de la palabra en inglés Mean Time to Repair. En español significa Tiempo Medio de Reparación. Así, el valor del MTTR representa el tiempo medio que se necesita para reparar una avería y que el equipo vuelva a su normal funcionamiento.

El tiempo promedio de remediación (MTTR) para una vulnerabilidad crítica en una aplicación web es de 35 días.

El MTTR para una vulnerabilidad de severidad crítica en un host o entorno en la nube con exposición a internet es de 61 días.



MTTR basado en EPSS vs MTTR basado en CVSS

Actualmente no está claro si las vulnerabilidades se resuelven más rápidamente en función de los puntajes de CVSS o EPSS. Existe una correlación débil entre EPSS y CVSS, pero no es lineal. En los próximos años, observar el MTTR en comparación con EPSS y CVSS indicará si EPSS está ganando más tracción en la industria.

EPSS	MTTR (Days)	CVSS	MTTR (Days)
>0.8	61.55	>9.0	45.46
0.5 to 0.79	56.68	7.5 to 8.9	55.56
0.3 to 0.49	75.98	6.0 to 7.4	59.92
0.1 to 0.29	43.84	3.0 to 5.9	61.33
0.1 to >0.99	62.5	1.0 to 2.9	50.32

>0.8	61.55 DAYS	>9.0	45.46 DAYS
0.5 to 0.79	56.68 DAYS	7.5 to 8.9	55.56 DAYS
0.3 to 0.49	75.98 DAYS	6.0 to 7.4	59.52 DAYS
0.1 to 0.29	43.84 DAYS	3.0 to 5.9	61.33 DAYS
0.1 to >0.99	62.5 DAYS	1.0 to 2.9	50.32 DAYS

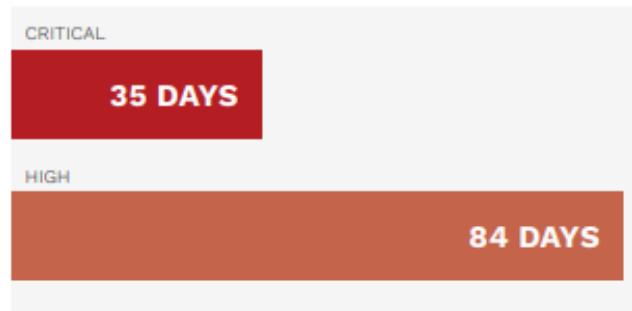


MTTR Aplicaciones Web

¿Qué tan rápido estamos abordando las vulnerabilidades en aplicaciones web en función de su severidad?

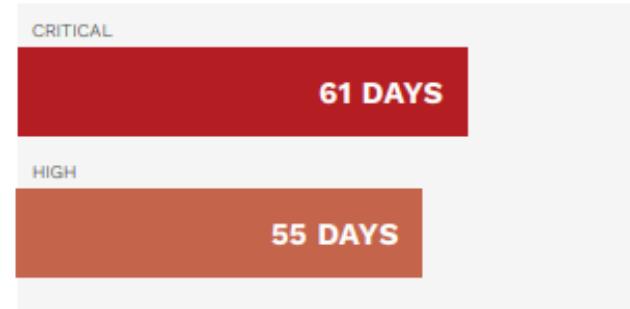
Severity	CVSS V2.0 RATINGS	CVSS V3.0 RATINGS
	Range	Range
LOW	0.0-3.9	0.1-3.9
MEDIUM	4.0-6.9	4.0-6.9
HIGH/CRITICAL	7.0-10.0	7.0-8.9

MTTR
Web Applications



MTTR Host/Network

MTTR
Network/Host – Internet Facing

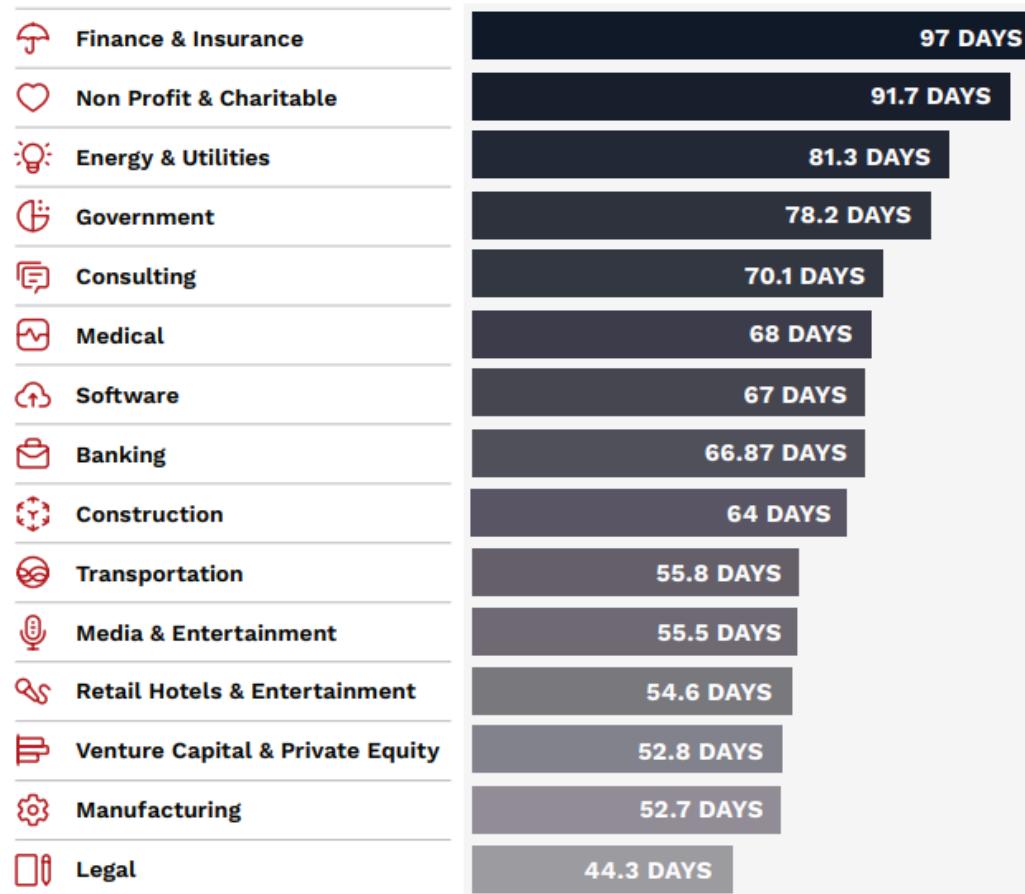


MTTR
Network/Host – Non Internet Facing



MTTR según la industria.

En 2023, examinamos quince industrias diferentes para informar sobre sus tasas promedio de MTTR dentro de cada sector. Podemos ver que el MTTR más corto se observa en el sector legal con 44 días, mientras que el más largo corresponde a Finanzas y Seguros con 97 días.





Vulnerabilidad de Red/Host más Común.

POR INDUSTRIA
CVSS >7.0

Industry	Vulnerability	CVE	CVSS	EPSS	Exploit Code Available
Microphone icon Media & Entertainment	Wowza Streaming Engine – Multiple Log4j Vulnerabilities (Log4Shell)	CVE-2021-44228, CVE-2021-45046	10	0.97454	
Document icon Legal	Microsoft Message Queuing (MSMQ) – RCE Vulnerability	CVE-2023-21554	10	0.96122	
Umbrella icon Finance & Insurance	Intel Active Management Technology – Multiple Vulnerabilities (INTEL-SA-00610)	CVE-2021-33159, CVE-2022-26845, CVE-2022-27497, CVE-2022-29893	9.8	0.00125	
Key icon Retail Hotels & Entertainment	VNC Brute Force Login	-	9	-	
Clipboard icon Venture Capital & Private Equity	Microsoft Exchange Server OWA – Multiple Vulnerabilities	CVE-2022-41040, VE-2022-41082	8.8	0.96949	Yes
Gear icon Manufacturing	SUSE: Security Advisory (SUSE-SU-2022:4240-1)	CVE-2022-43995	8.8	0.0045	
Heart icon Non Profit & Charitable	Microsoft SQL Server – Multiple RCE Vulnerabilities	CVE-2023-21528, CVE-2023-21704, CVE-2023-21705, CVE-2023-21713, CVE-2023-21718	8.8	0.00259	

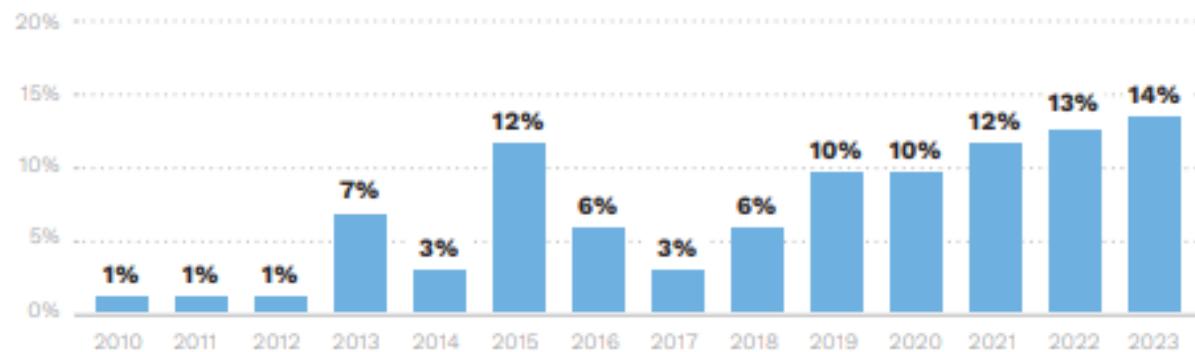


Vulnerabilidad de Red/Host más Común.

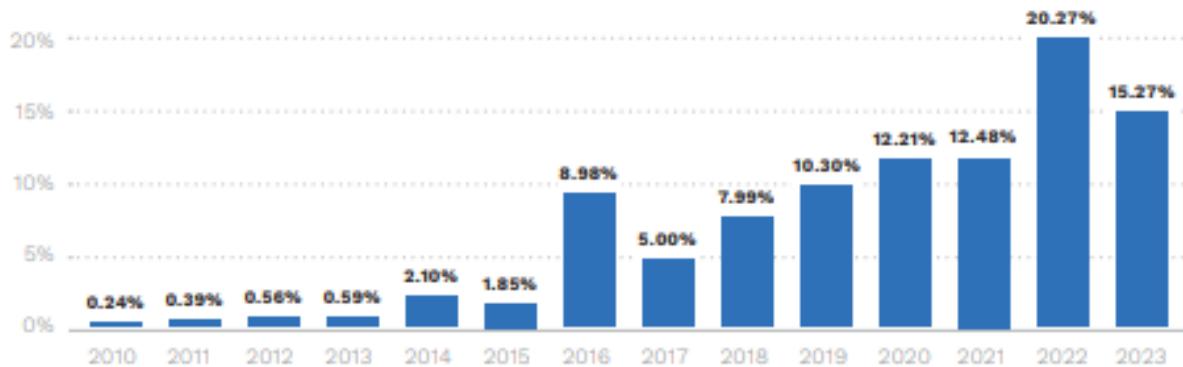
Government	Windows IExpress – Untrusted Search Path Vulnerability	CVE-2018-0598	7.8	0.00846	
Medical	OpenSSH – Command Injection Vulnerability	CVE-2020-15778	7.8	0.00289	
Consulting	SNMP Agent Default Community Names	CVE-1999-0517	7.5	0.45448	
Construction	SNMP Agent Default Community Names	CVE-1999-0517	7.5	0.45448	
Banking	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	CVE-2016-2183	7.5	0.00547	Yes
Energy & Utilities	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	CVE-2016-2183	7.5	0.00547	Yes
Software	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	CVE-2016-2183	7.5	0.00547	Yes
Transportation	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	CVE-2016-2183	7.5	0.00547	Yes

Vulnerabilidades Descubiertas por Edad.

Vulnerabilities Discovered by Age



Vulnerabilities >CVSS 7.0 by Age

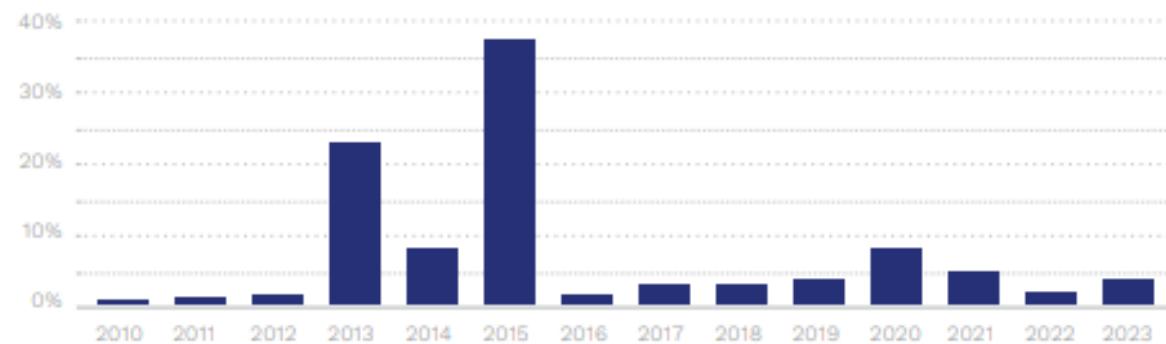


El 45% de las vulnerabilidades descubiertas tenían entre 1 y 4 años. Esta métrica puede parecer deficiente si no se considera la severidad o el puntaje de CVSS.

Cuando observamos las vulnerabilidades por edad para aquellas con un CVSS >7.0, vemos que el 55% tiene entre 1 y 4 años.

Vulnerabilidades Descubiertas por Edad.

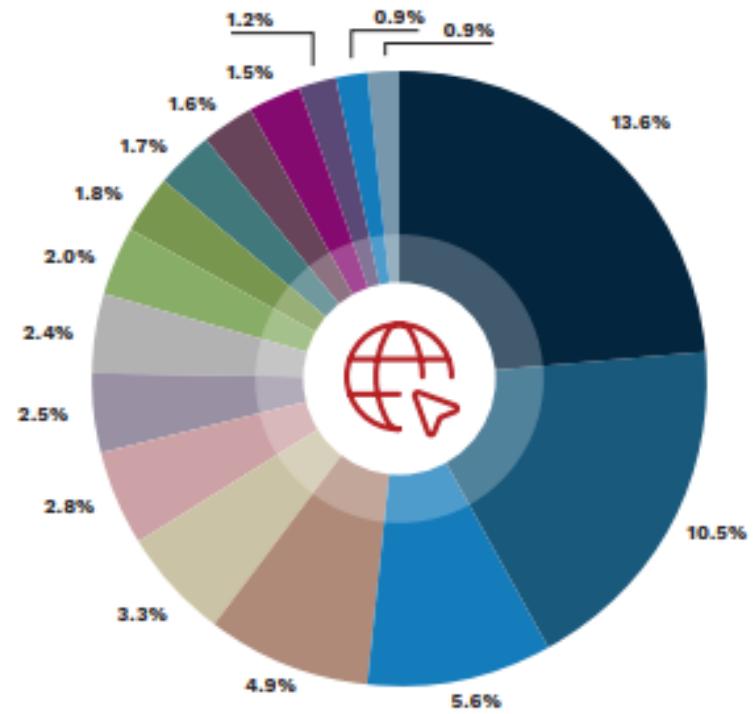
Vulnerabilities <EPSS 0.7 by Age



El aumento en 2015 se debe a las vulnerabilidades de criptografía (CVE) que tienen un EPSS > 0.7, de las cuales hay muchas.

Gestión de la Superficie de Ataque (ASM).

Basado en una muestra de 2,000,000 de escaneos de endpoints, a continuación se describen los puertos expuestos, su tasa de ocurrencia y la razón para no exponerlos a Internet público si es posible.

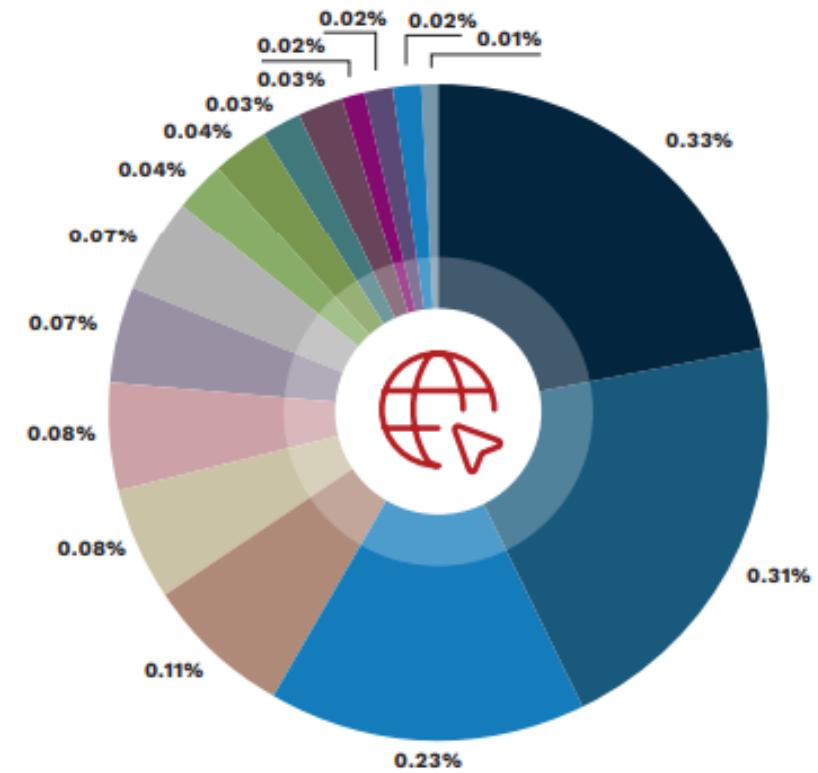


Gestión de la Superficie de Ataque (ASM).

Port	Protocol	Count	% Occurance	Description	Notes
443	tcp	134160	13.6%	TLS/HTTPS Port	-
80	tcp	103560	10.5%	HTTP Port	-
161	udp	54680	5.6%	SNMP	There are 489 CVE's related to this protocol
1720	tcp	47800	4.9%	H. 323 teleconferencing protocol	There are 40 CVE's related to this protocol
500	udp	32920	3.3%	Internet key exchange (IKE) /VPN	There are 158 CVE's related to this protocol
22	tcp	27360	2.8%	SSH (Secure Shell) protocol	There are 973 CVE's related to this protocol
5060	tcp	24240	2.5%	SIP Protocol	There are 509 CVE's related to this protocol
2000	tcp	23120	2.4%	SSCP Protocol	-
8443	tcp	20040	2.0%	HTTPS	Development HTTP port or Proxy Server
541	tcp	17480	1.8%	FortiManager and FortiGate Cloud Management	There are 79 CVE's related to this protocol
8080	tcp	16960	1.7%	HTTP Port	Development HTTP port or Proxy Server
123	udp	15520	1.6%	NTP server communication	There are 161 CVE's related to this protocol
1723	tcp	15040	1.5%	Point-to-Point Tunneling Protocol (PPTP)	There are 66 CVE's related to this protocol
23	tcp	11440	1.2%	Telnet protocol	Unencrypted Protocol! There are 535 CVE's related to this protocol
8000	tcp	8560	0.9%	HTTP (Development env)	Possible development HTTP port

Gestión de la Superficie de Ataque (ASM) – ¡Puertos Malos!

Basado en una muestra de 2,000,000 de escaneos de endpoints, a continuación se describen los puertos expuestos, su tasa de ocurrencia y la razón para no exponerlos a Internet público si es posible.

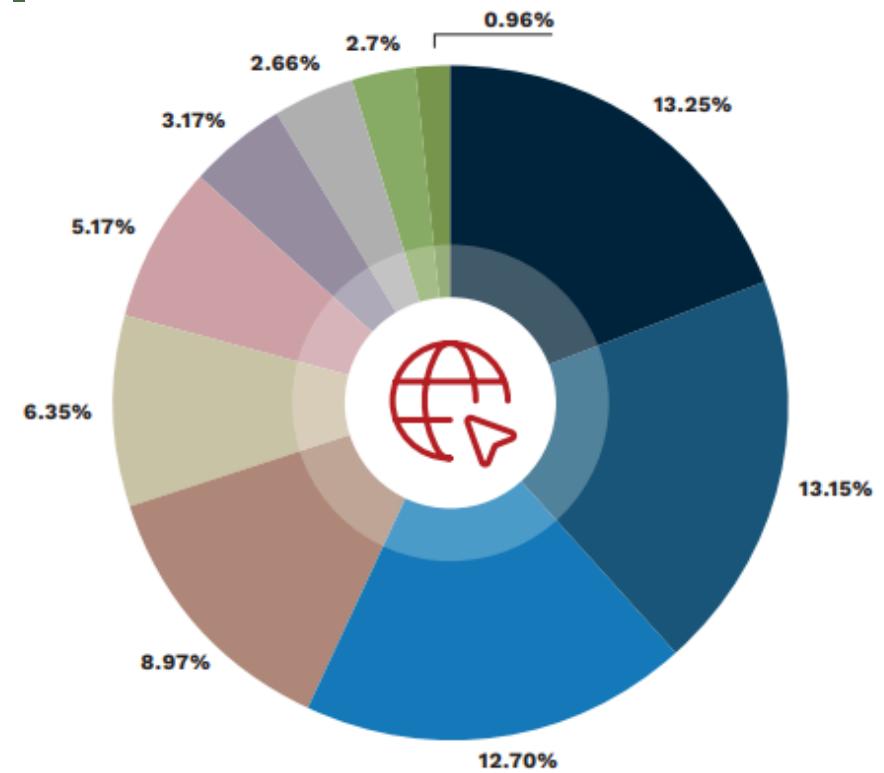


Gestión de la Superficie de Ataque (ASM) – ¡Puertos Malos!

Port	Protocol	Count	% Occurrence	Description	Notes
7000	tcp	3240	0.33%	Exposed Cassandra Database Port	Exposed Database ports are trouble!
21	tcp	3040	0.31%	Ports 20 and 21: These are TCP-only ports used for FTP (File Transfer Protocol).	FTP is outdated and insecure, making these ports susceptible to attacks like anonymous authentication, cross-site scripting, password brute force, or directory traversal.
3389	tcp	2280	0.23%	Port 3389: This is the Remote Desktop Protocol (RDP) port. It allows remote access to a system.	If not properly secured, it can be exploited by attackers
3306	tcp	1120	0.11%	Ports 1433, 1434, and 3306: These are the default ports for SQL Server and MySQL.	They are often targeted for malware distribution. Ensure proper security measures if you use these ports.
445	tcp	800	0.08%	Port 445 (SMB): This port provides file and printer sharing capabilities.	Unfortunately, it was infamously used in the 2017 WannaCry ransomware attack. Be cautious when dealing with this port.
5900	tcp	800	0.08%	Port 5900 (VNC): The Virtual Network Computing (VNC) port allows remote desktop access.	If not secured properly, it can be exploited by attackers.
9100	tcp	680	0.07%	Port 9100 (JetDirect): Used for printer communication	It can be a target for unauthorized printing or even attacks on the printer itself.
135	tcp	640	0.07%	Port 135 (MS RPC): The Microsoft Remote Procedure Call (RPC) service is used for communication between Windows systems.	It has been exploited in the past for worms and malware. If not needed, consider blocking this port.
1433	tcp	360	0.04%	Ports 1433, 1434, and 3306: These are the default ports for SQL Server and MySQL.	They are often targeted for malware distribution. Ensure proper security measures if you use these ports.

Vulnerabilidades con Riesgo Aceptado.

Vulnerabilidades más comunes que están marcadas como "Riesgo Aceptado" en la plataforma EdgeScan por las propias organizaciones.



Vulnerabilidades de riesgo aceptadas

Vulnerability Name	% of Total	CVE	CVSS	EPSS	CISA KEV
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	13.25%		3.7	0	FALSE
Weak Host Key Algorithm(s) (SSH)	13.15%		3.7	0	FALSE
Weak Public Key Size (SSH)	12.70%		3.7	0	FALSE
TLS Version 1.1 Protocol Detection	8.97%		6.5	0	FALSE
SNMP Agent Default Community Names	6.35%	CVE-1999-0517	7.5	0.45448	FALSE
SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing	5.17%		6.5	0	FALSE
Xerox Printers DoS Vulnerability (XRX22-002)	3.17%	CVE-2022-23968	7.5	0.00163	FALSE
Anonymous FTP Enabled	2.66%	CVE-1999-0497	5.3	0.1987	FALSE
Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6)	2.17%	CVE-2021-34428	3.5	0.00107	FALSE
Oracle Database Server < 19.1 Multiple Vulnerabilities (cpuapr2020)	0.96%	CVE-2021-41182, CVE-2021-41183, CVE-2021-41184, CVE-2022-24728, CVE-2022-24729	7.5	0.00311	FALSE

CISA KEV (Catalog of Known Exploited Vulnerabilities) es una lista mantenida por la CISA (Agencia de Seguridad Cibernética e Infraestructura de EE. UU.) que agrupa las vulnerabilidades conocidas que han sido explotadas activamente. Si un CVE (Common Vulnerabilities and Exposures) aparece en esta lista, significa que ha sido reconocido como un riesgo activo.

EPSS (Exploit Prediction Scoring System) es una puntuación que estima la probabilidad de que una vulnerabilidad sea explotada en el futuro. Cuando se refiere a varias vulnerabilidades, se toma el valor más alto como referencia para medir el riesgo.

Vulnerabilidades de riesgo aceptadas

Vulnerability Name	% of Total	CVE	CVSS	EPSS	CISA KEV
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	13.25%		3.7	0	FALSE
Weak Host Key Algorithm(s) (SSH)	13.15%		3.7	0	FALSE
Weak Public Key Size (SSH)	12.70%		3.7	0	FALSE
TLS Version 1.1 Protocol Detection	8.97%		6.5	0	FALSE
SNMP Agent Default Community Names	6.35%	CVE-1999-0517	7.5	0.45448	FALSE
SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing	5.17%		6.5	0	FALSE
Xerox Printers DoS Vulnerability (XRX22-002)	3.17%	CVE-2022-23968	7.5	0.00163	FALSE
Anonymous FTP Enabled	2.66%	CVE-1999-0497	5.3	0.1987	FALSE
Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6)	2.17%	CVE-2021-34428	3.5	0.00107	FALSE
Oracle Database Server < 19.1 Multiple Vulnerabilities (cpuapr2020)	0.96%	CVE-2021-41182, CVE-2021-41183, CVE-2021-41184, CVE-2022-24728, CVE-2022-24729	7.5	0.00311	FALSE

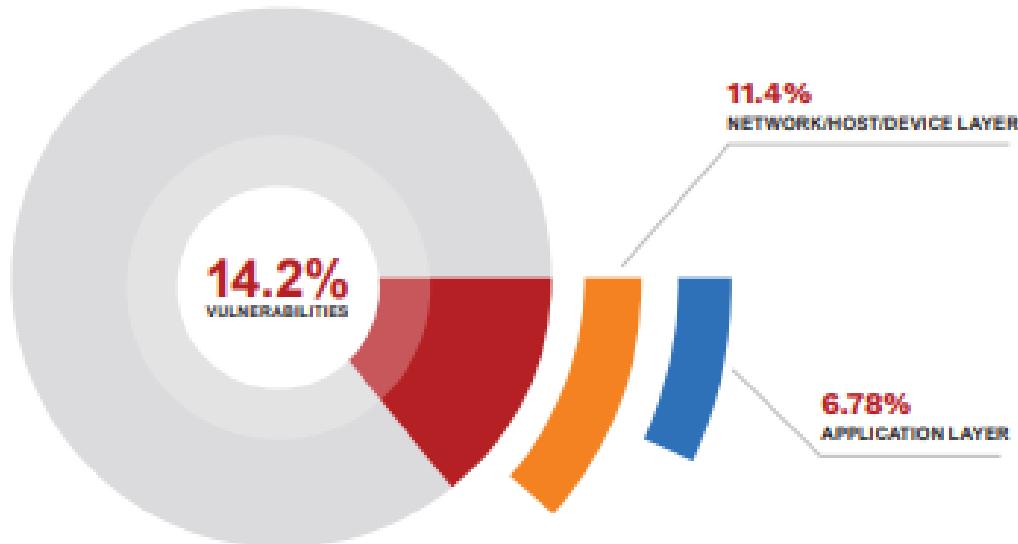
Los algoritmos de intercambio de claves débiles (Weak Key Exchange, KEX) en SSH son vulnerables principalmente debido a la posibilidad de que un atacante pueda explotar debilidades criptográficas para interceptar o manipular las comunicaciones cifradas. Algunas de las vulnerabilidades asociadas a estos algoritmos son:

Vulnerabilidades de riesgo aceptadas

Vulnerability Name	% of Total	CVE	CVSS	EPSS	CISA KEV
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	13.25%		3.7	0	FALSE
Weak Host Key Algorithm(s) (SSH)	13.15%		3.7	0	FALSE
Weak Public Key Size (SSH)	12.70%		3.7	0	FALSE
TLS Version 1.1 Protocol Detection	8.97%		6.5	0	FALSE
SNMP Agent Default Community Names	6.35%	CVE-1999-0517	7.5	0.45448	FALSE
SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing	5.17%		6.5	0	FALSE
Xerox Printers DoS Vulnerability (XRX22-002)	3.17%	CVE-2022-23968	7.5	0.00163	FALSE
Anonymous FTP Enabled	2.66%	CVE-1999-0497	5.3	0.1987	FALSE
Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6)	2.17%	CVE-2021-34428	3.5	0.00107	FALSE
Oracle Database Server < 19.1 Multiple Vulnerabilities (cpuapr2020)	0.96%	CVE-2021-41182, CVE-2021-41183, CVE-2021-41184, CVE-2021-41185, CVE-2022-24729	7.5	0.00311	FALSE

las vulnerabilidades en las API y aplicaciones web suelen ser reparadas de forma eficiente, la mayoría de los problemas graves de seguridad se encuentran en la red. Es decir, las fallas más peligrosas están en la infraestructura de red, no tanto en las aplicaciones web o API.

Acumulación de vulnerabilidades



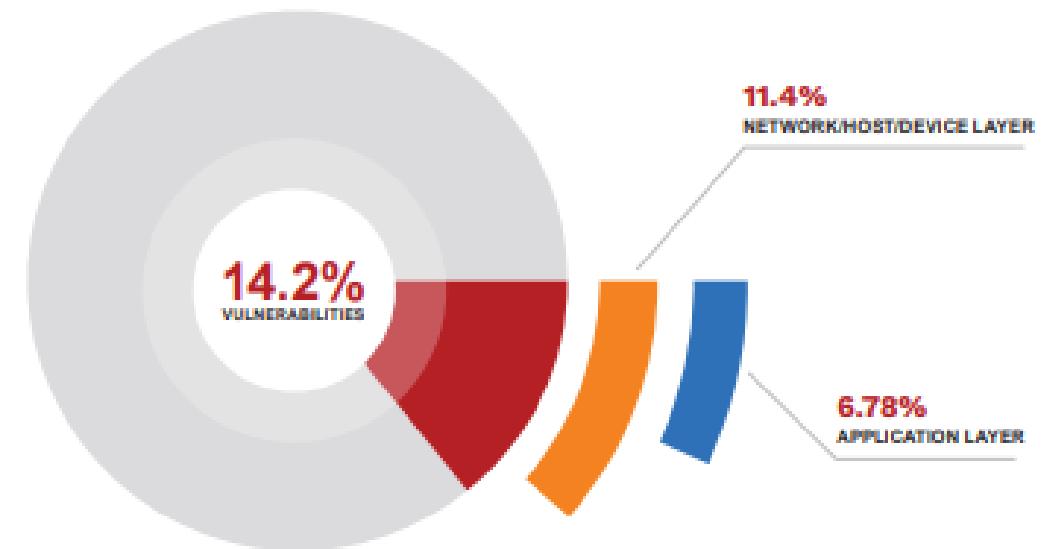
La mayoría de las vulnerabilidades más graves en una empresa no se encuentran en las aplicaciones o APIs (programas), sino en la red o dispositivos, y representan un riesgo significativo si no se solucionan. El gráfico también muestra que, en promedio, las empresas grandes dejan sin resolver casi la mitad de las vulnerabilidades detectadas.

Acumulación de vulnerabilidades

14.2% de las vulnerabilidades no resueltas son graves o críticas: Esto significa que en una empresa, el 14.2% de las vulnerabilidades descubiertas en el último año son muy peligrosas y podrían causar serios problemas si no se arreglan.

11.4% de estas vulnerabilidades graves se encuentran en la red, host o dispositivos: La mayoría de las vulnerabilidades graves (11.4%) están relacionadas con equipos de red, servidores o dispositivos que usa la empresa, lo que puede afectar el funcionamiento general de la infraestructura de TI.

6.78% están en la capa de aplicación, una pequeña parte de las vulnerabilidades graves (6.78%) afecta directamente a las aplicaciones, como los sitios web o programas que usa la empresa.



Agrupación de vulnerabilidades

Vulnerabilidad con EPSS Score:

3.42%

1.72%

Probabilidad de Brecha:

3/100

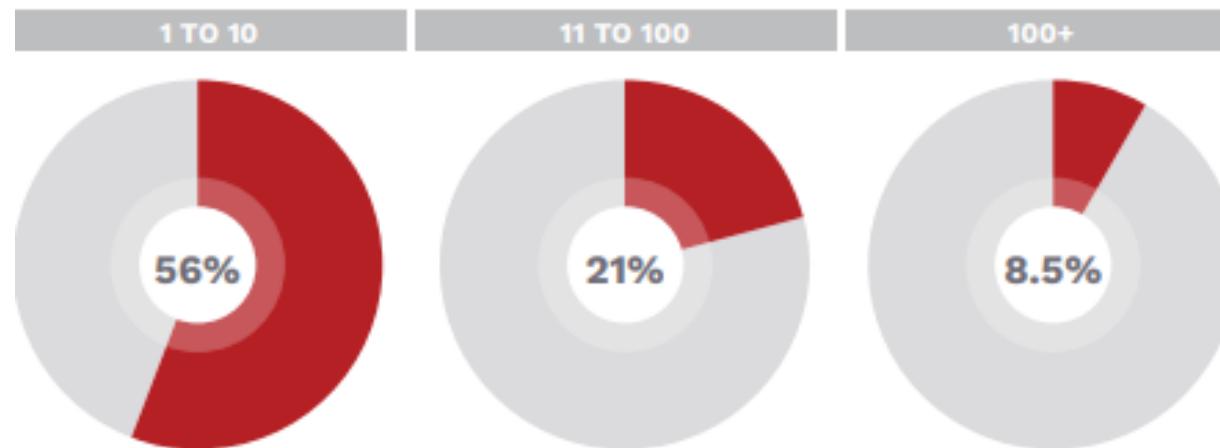
2/100

- 3.42% de todos los activos tienen al menos 1 vulnerabilidad con una puntuación EPSS mayor a 0.7.
- EPSS es una puntuación que predice la probabilidad de que una vulnerabilidad sea explotada.
- 1.72% de todos los activos tienen al menos 10 vulnerabilidades con una puntuación EPSS mayor a 0.7

- 3/100 (3 de cada 100 activos) tienen al menos 1 vulnerabilidad con una probabilidad de brecha (ser explotado) de al menos el 70%.
- 2/100 (2 de cada 100 activos) tienen más de 10 vulnerabilidades con una probabilidad de brecha de al menos el 70%.

Agrupación de vulnerabilidades

Vulnerability Count (Cantidad de vulnerabilidades por activo):



- 56% de los activos evaluados en 2023 tenían entre 1 y 10 vulnerabilidades durante el año.
- 21% de los activos evaluados tenían entre 11 y 100 vulnerabilidades.
- 8.5% de los activos tenían más de 100 vulnerabilida

Above we can see:

56%

OF ALL ASSETS ASSESSED IN 2023 HAD BETWEEN 1 AND 10 VULNERABILITIES THROUGHOUT THE 12 MONTH PERIOD

21%

OF ALL ASSETS ASSESSED IN 2023 HAD BETWEEN 11 AND 100 VULNERABILITIES & 8.5% OF ASSETS HAD 100+ VULNERABILITIES

La mayoría de los activos tienen varias vulnerabilidades. Más de la mitad (56%) tienen entre 1 y 10 vulnerabilidades, mientras que un número más pequeño tiene muchas más (por ejemplo, 8.5% con más de 100). Algunas vulnerabilidades son más graves y tienen una alta probabilidad de ser explotadas.