



2024

Vulnerability Statistics Report

9th Edition



Introduction & Synopsis

Welcome to the 9th edition of the Edgescan Vulnerability Stats Report 2024.

This report demonstrates the state of full stack security based on thousands of security assessments and penetration tests on millions of assets that were performed globally from the Edgescan Cybersecurity Platform in 2023.

This is an analysis of vulnerabilities detected in the systems of hundreds of organizations across a wide range of industries – from the Fortune 500 to medium and small businesses.

The report provides a statistical model of the most common weaknesses faced by organizations to enable data-driven decisions for managing risks and exposures more effectively.

We hope this report will provide a unique by-the-numbers insight into trends, statistics and a snapshot of the overall state of cybersecurity for the past year, from the perspective of vulnerabilities discovered and remediated, as well as penetration testing success rates.

We are proud that this yearly report has become a reliable source for approximating the global state of vulnerability management. This is exemplified by our unique dataset being part of the Verizon Data Breach Investigations Report (DBIR), which is the de facto standard for insights into the common drivers for incidents and breaches today.

This year we delve into Risk Density to describe where critical severity vulnerabilities and exposures are clustered in the IT technical stack, quantification of attack surface management exposures and risks, and Mean Time To Remediate (MTTR) critical vulnerabilities.

We split our statistical models across layers of the technology stack (Full Stack) such as Web Application, API, and Device/Host layers.

Additionally, we make a distinction in the data, highlighting if discovered CVE's have associated exploit code freely available.

Unfortunately, we still see high rates of known (patchable) exploitable vulnerabilities, with working exploits in the wild being used by nation states and cyber criminal groups against organizations who are slow to patch.

Since Edgescan employs a number of risk prioritization scoring mechanisms, we take a deeper look at the most common risks faced by organizations and also look at correlation of the various risk scoring methodologies.

Some of the results are surprising and we hope you will stay to the end to learn more!

Given Edgescan maps validated vulnerabilities automatically to CVSS¹ (Common Vulnerability Scoring System), CISA KEV² (Cyber Security & Infrastructure Security Agency Known Exploited Vulnerability Catalogue), EPSS³ (Exploit Prediction Scoring System) and our own EVSS (Edgescan Validated Security Score), we have leveraged this information to provide a qualitatively better guide to what the most common risks are, as faced by systems deployed in modern enterprises.

1. www.first.org/cvss/

2. www.cisa.gov/known-exploited-vulnerabilities

3. www.first.org/epss/

Contents

Introduction & Synopsis	2
Welcome	4
2023 – Year in Review	6
Vulnerability Severity EPSS, CISA KEV & EVSS	8
Risk Density	9
PCI Failures Per Severity	10
Most common High & Critical Severity by CWE – Web Applications	11
Most common High & Critical Severity Web Application Vulnerabilities	12
CISA KEV	14
Most Common Vulnerability with EPSS >0.8 Public Internet Facing	15
Most Common Vulnerability with EPSS >0.8 Non-Public Internet Facing	16
Most Common High & Critical Severity (CVSS) – Non-Internet Facing	18
Most Common High & Critical Severity (CVSS) – Public Internet Facing	19
MTTR* based on EPSS Vs MTTR based on CVSS	21
MTTR Web Application	22
MTTR Host/Network	22
MTTR Per Industry	23
Most Common Network/Host Vulnerability – Per Industry CVSS >7.0	25
Most Common Network/Host Vulnerability – Per Industry > Medium Severity	26
Vulnerabilities Discovered By Age	27
Attack Surface Management (ASM)	28
Attack Surface Management (ASM) – Bad Ports!	29
Risk Accepted Vulnerabilities	30
Vulnerability Backlog	31
Vulnerability Clustering	32
Conclusion	33
What Is Edgescan	34

* Mean Time to Remediation

Welcome

When we examine cyber posture from an attack surface standpoint, exposed services are a real risk.

Statistically some vulnerabilities have a very low frequency of occurrence compared to the total number of vulnerabilities discovered, but many will result in a breach with an outsized impact, which we can call an intensive rather than extensive risk.

Similarly to the 2023 report, patching and maintenance is a challenge and we still find that it is not trivial to patch production systems.

The MTTR (Mean Time to Remediation) stats also reflect on this issue. Continuous detection and assessment needs improvement and as I've always said, visibility is paramount.

Internal, non-public cyber security posture is significantly lacking in terms of resilience and ease of exploit. Combining vulnerabilities across the stack, in some cases, results in the potential impact being much more severe than the sum of the individual discovered vulnerabilities.

Oddly, CVE's dating from 2015 are still being discovered and are being used by ransomware and malware toolkits to exploit systems when they can find them.

Attack Surface Management (Visibility) is a key driver to cybersecurity best practices and based on our continuous asset profiling, we discuss how common sensitive and critical systems are exposed to the public Internet far more than they should be.

The assumption here is that enterprises simply do not have systems, people and processes in place, to make them aware of exposures in a manner that facilitates remediation actions.

This report provides a global snapshot across dozens of industry verticals and how to prioritize what is important, as not all vulnerabilities are created equal.

Best regards,



Eoin Keary

Founder,
Edgescan.
com

INSIGHT FROM THIS REPORT...

Across the full stack **MORE THAN 33%** of discovered vulnerabilities were of a critical or high severity.

WHO IS FULLSTACK?

A PILLAR OF THE INTERNET. NEITHER A VILLAIN OR A HERO BUT OBSERVES THE BATTLEFIELD. HAS BEEN GROWING IN COMPLEXITY AND SIZE SINCE THE INTERNET BEGAN AND IS CONSIDERED A GOD-LIKE ENTITY IN THE CYBER-UNIVERSE. FULLSTACK IS VITALLY IMPORTANT TO THE HEROES TO ENSURE THE WEB IS SAFE!



2023 – Year in Review

VULNERABILITIES OF NOTE IN 2023

The list below depicts some of the more “popular” CVEs leveraged by threat actors in 2023. As can be seen, it is a rogues’ gallery of both web application and native software vulnerabilities, which are commonly found across most organizations.

CVE-2023-34362: A severe SQL injection vulnerability in MOVEit Transfer, exploited in Cl0p Ransomware attacks affecting millions.

Root cause: Web application vulnerability, SQL Injection attack. Poor development practices.

CVSS: 9.8 **EPSS:** 95.5% **CISA KEV:** True

CVE-2023-0669: An RCE vulnerability in Fortra GoAnywhere MFT, leading to a significant increase in ransomware attacks by groups such as ALPHV (BlackCat) and LockBit.

Root cause: Web application vulnerability, Remote Command Injection Attack. Poor development practices, poor validation, encoding and design.

CVSS: 7.2 **EPSS:** 96.8% **CISA KEV:** True

CVE-2023-27350: An Improper Access Control vulnerability in PaperCut, exploited by Cl0p and Bl00dy Ransomware.

Root cause: Web application vulnerability, Weak authorization logic. Poor development practices, poor QA, Difficult to detect with automated testing/tools.

CVSS: 9.8 **EPSS:** 97.23% **CISA KEV:** True

CVE-2023-24880: A Windows SmartScreen Security Feature Bypass vulnerability, exploited by ransomware actors.

Root cause: Application vulnerability, Weak authorization logic. Poor development practices, Poor QA, Difficult to detect with automated testing/tools.

CVSS: 4.4 **EPSS:** 0.55% **CISA KEV:** True

CVE-2023-28252: A Windows CLFS Driver vulnerability for Privilege Escalation, exploited in distributing Nokoyawa Ransomware.

Root cause: Application vulnerability, Weak authorization logic. Poor development practices, Poor QA, Difficult to detect with automated testing/tools.

CVSS: 7.8 **EPSS:** 1.82% **CISA KEV:** True

CVE-2023-29059: A vulnerability in the 3CX VoIP desktop client, exploited for arbitrary code execution in ransomware attacks through compromised software updates.

Root cause: Command Injection Attack. Poor development practices, poor validation, encoding and design.

CVSS: 7.8 **EPSS:** 0.06% **CISA KEV:** True

CVE-2023-2868: A critical remote command injection flaw in Barracuda Email Security Gateway, allowing attackers significant control and manipulation capabilities.

Root cause: Command Injection Attack. Poor development practices, poor validation, encoding and design.

CVSS: 9.4 **EPSS:** 5.35% **CISA KEV:** True

CVE-2023-23397: A Microsoft Outlook Elevation of Privilege Vulnerability, allowing attackers to bypass authentication measures.

Root cause: Application vulnerability, Weak authorization logic. Poor development practices, Poor QA, Difficult to detect with automated testing/tools.

CVSS: 9.8 **EPSS:** 91.73% **CISA KEV:** True

2023 – Year in Review

MOST SIGNIFICANT BREACHES IN 2023

In 2023, several significant cyber breaches occurred, impacting millions of individuals and organizations worldwide. Some of the largest breaches include:

**ICMR (Indian Council of Medical Research):**

This breach involved the personal data of 815 million Indian residents, apparently exfiltrated from the ICMR's Covid-testing database. The data included names, ages, genders, addresses, passport numbers, and Aadhaar numbers.

.18 Darkbeam

DarkBeam: A digital risk protection firm, exposed 3.8 billion records due to a misconfigured Elasticsearch and Kibana interface. Although most records came from previous breaches, the exposed data could facilitate phishing campaigns.



SAP SE Bulgaria: Researchers discovered Kubernetes Secrets related to hundreds of organizations exposed in public GitHub repositories, including SAP SE, exposing 95,592,696 records/artifacts.

TmaxSoft

TmaxSoft: An IT company in South Korea, exposed 2 TB of data, including over 56 million sensitive records, via a Kibana dashboard for more than two years.



Anonymous Sudan: A hacktivist group conducted DDoS attacks against large tech firms, including Microsoft's Outlook, OneDrive, and Azure portal. These attacks demonstrated the capability to impact major tech infrastructure.

PayPal

PayPal: Experienced a credential stuffing attack that compromised 34,942 accounts, exposing personal information such as names, addresses, and social security numbers (14†source).



DISH Network: Went offline due to a ransomware attack by the Black Basta ransomware gang, affecting websites, mobile apps and internal systems.



GoDaddy: Suffered a multi-year breach where attackers stole source code and installed malware, affecting 1.2 million Managed WordPress customers.



MGM Resorts International: Was hit by a massive cyberattack that impacted systems across its properties, attributed to the BlackCat ransomware operation.



3CX: Experienced a breach by the North Korean Lazarus hacking group through a supply chain attack, compromising the 3CX Phone System used by over 350,000 companies worldwide.



Barracuda: Announced that their Email Security Gateway (ESG) appliances were hacked using a zero-day vulnerability, leading to a recommendation that impacted ESG appliances be immediately replaced.



ESXiArgs ransomware attack: Targeted VMware ESXi servers globally, encrypting virtual machines for thousands of companies.

These breaches highlight the diversity of cyber threats, from database exposures and ransomware attacks to supply chain vulnerabilities and DDoS attacks. They underscore the importance of cybersecurity measures, including secure configurations, vigilant monitoring and prompt incident response strategies.

Vulnerability Severity EPSS, CISA KEV & EVSS

What is EPSS?

The Exploit Prediction Scoring System (EPSS) is an open, data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

<https://www.first.org/epss/>

What is CISA KEV?

CISA (Cybersecurity & Infrastructure Security Agency) maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalog. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

<https://www.cisa.gov/known-exploited-vulnerabilities>

Edgescan Validated Security Score (EVSS)

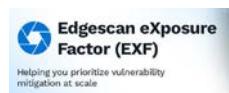
Every vulnerability discovered by Edgescan is validated via a combination of advanced “big-data” analytics and human expertise, resulting in near false positive-free vulnerability intelligence. Once a vulnerability is validated it is mapped to both the CISA KEV and EPSS to assist with prioritization. All vulnerabilities in Edgescan (where applicable) have a EPSS, CISA KEV, CVSS and EVSS risk score.

<https://www.edgescan.com/solutions/risk-based-vulnerability-management-rbvm/>

Edgescan eXposure Factor (EXF)

The edgescan Exposure factor combines EPSS, CVSS, CISA KEV and EVSS to reach a simple priority score which taken in relevance with other vulnerabilities provides a simple way to prioritize discovered and validated vulnerabilities.

<https://www.edgescan.com/edgescan-exposure-factor-exf/>



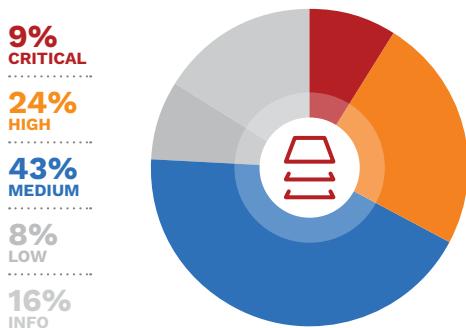
Risk Density

The following is a breakdown of vulnerabilities by severity, discovered across the full stack; Web Applications, API's and Network/Host deployments.

It also depicts the risks associated with potential PCI (Payment Card Industry) Failures – not every vulnerability results in a PCI fail. Severity is defined via the Edgescan Validated Security Score (EVSS). Later in the report we draw upon CVSS, CISA KEV and EPSS Risk and Probability scores.

Severity is based on Edgescan EVSS (Edgescan Validated Vulnerability Score). EVSS is applied to Web application vulnerabilities and is based upon likelihood & impact when a vulnerability is undergoing validation.

Severity Dispersion Across the Full Stack (Network, Web, API combined)

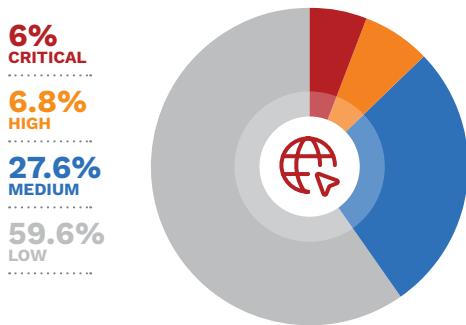


ACROSS THE FULL STACK MORE THAN 33% OF DISCOVERED VULNERABILITIES WERE OF A CRITICAL OR HIGH SEVERITY

SEVERITY IS BASED ON EDGESCAN EVSS (EDGESCAN VALIDATED VULNERABILITY SCORE)

EVSS IS APPLIED TO WEB APPLICATION VULNERABILITIES AND IS BASED UPON LIKELIHOOD & IMPACT WHEN A VULNERABILITY IS UNDERGOING VALIDATION

Web Application & API Vulnerability Dispersion by Severity

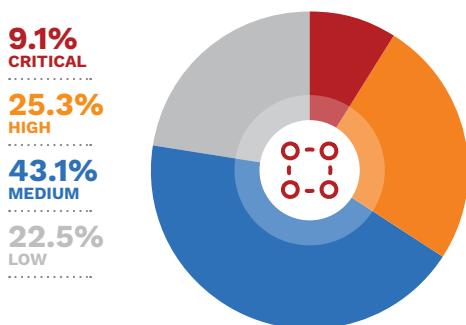


ACROSS THE WEB APPLICATION AND API LAYERS 12.8% OF DISCOVERED VULNERABILITIES WERE OF A CRITICAL OR HIGH SEVERITY

AS DEPICTED LATER IN THIS DOCUMENT CRITICAL AND HIGH SEVERITY VULNERABILITIES REMAIN VERY SIMILAR TO PREVIOUS YEARS

VULNERABILITIES SUCH AS SQL INJECTION (CWE-89) ARE READILY DISCOVERED AND ACCOUNT FOR 19.47% OF ALL CRITICAL AND HIGH SEVERITY VULNERABILITIES

Network/Host Vulnerability Dispersion by Severity



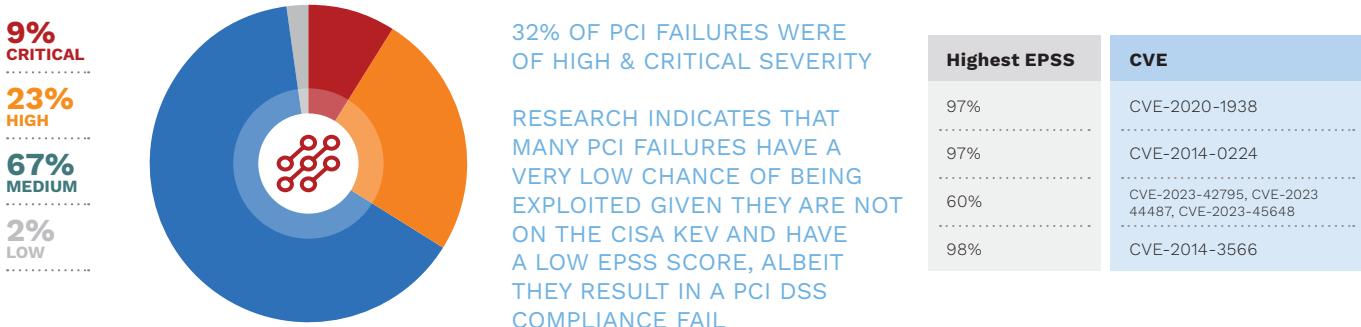
34.4% OF DISCOVERED VULNERABILITIES IN THE INFRASTRUCTURE/HOSTING/ CLOUD/NETWORK LAYER WERE OF A CRITICAL OR HIGH SEVERITY

19% HAD AN EPSS SCORE ABOVE 0.8 (PROBABILITY OF BREACH EXCEEDING 80%)

Breach Probability	Dispersion
EPSS > 0.8 (>80%)	19%
EPSS 0.6 - 0.79 (60%-79%)	1%
EPSS 0.1-0.59 (10% - 59%)	17%
EPSS below < 0.1 (10%)	63%

PCI Failures Per Severity

PCI Failures Per Severity



PCI Failures with an EPSS Score <10%

AN EPSS SCORE BELOW 0.10 DEPICTS THE PROBABILITY OF BREACH VIA SUCH A VULNERABILITY IS LESS THAN 10%

Name	% of Total PCI Fails	Layer	CWEs	CVEs	On CISA List	PCI Status	CVSS Score	EPSS Score	Network Access
OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)	8%	network		CVE-2016-20012	FALSE	fail	5.3	0.00369	external
OpenSSH <= 8.6 Command Injection Vulnerability	8%	network	CWE-78	CVE-2020-15778	FALSE	fail	7.8	0.00289	external
OpenBSD OpenSSH < 9.3p2 RCE Vulnerability	7%	network	CWE-428	CVE-2023-38408	FALSE	fail	9.8	0.04189	external
SSL/TLS: BREACH Attack Against HTTP Compression	6%	network	CWE-200	CVE-2013-3587	FALSE	fail	5.9	0.00334	external
PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux	4%	network	CWE-125, CWE-190	CVE-2022-31630, CVE-2022-37454	FALSE	fail	9.8	0.01015	external
OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability	4%	network	CWE-269	CVE-2021-41617	FALSE	fail	7	0.00055	external
OpenSSH < 8.1 Integer Overflow Vulnerability	3%	network	CWE-190	CVE-2019-16905	FALSE	fail	7.8	0.00048	external
Python < 3.10.6 Information Disclosure Vulnerability (bpo-43223) - Linux	3%	network	CWE-601	CVE-2021-28861	FALSE	fail	7.4	0.00187	internal
SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	1%	network	CWE-200	CVE-2016-2183	FALSE	fail	7.5	0.00547	internal
ISC BIND Multiple Vulnerabilities (Feb 2019) - Linux	1%	network	CWE-327, CWE-732, CWE-772	CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	FALSE	fail	7.5	0.02516	external

The most common PCI failures with a probability of breach below 10%

As above, 8% of all PCI fails relate to CVE-2016-20012 which has an EPSS of 0.04% which is very low.

The question to ponder: even though this issue will result in a PCI compliance fail, should we really be focusing resources on fixing other issues which are more likely to be exploited, rather than those that are currently not?

Most Common High & Critical Severity By CWE – Web Applications

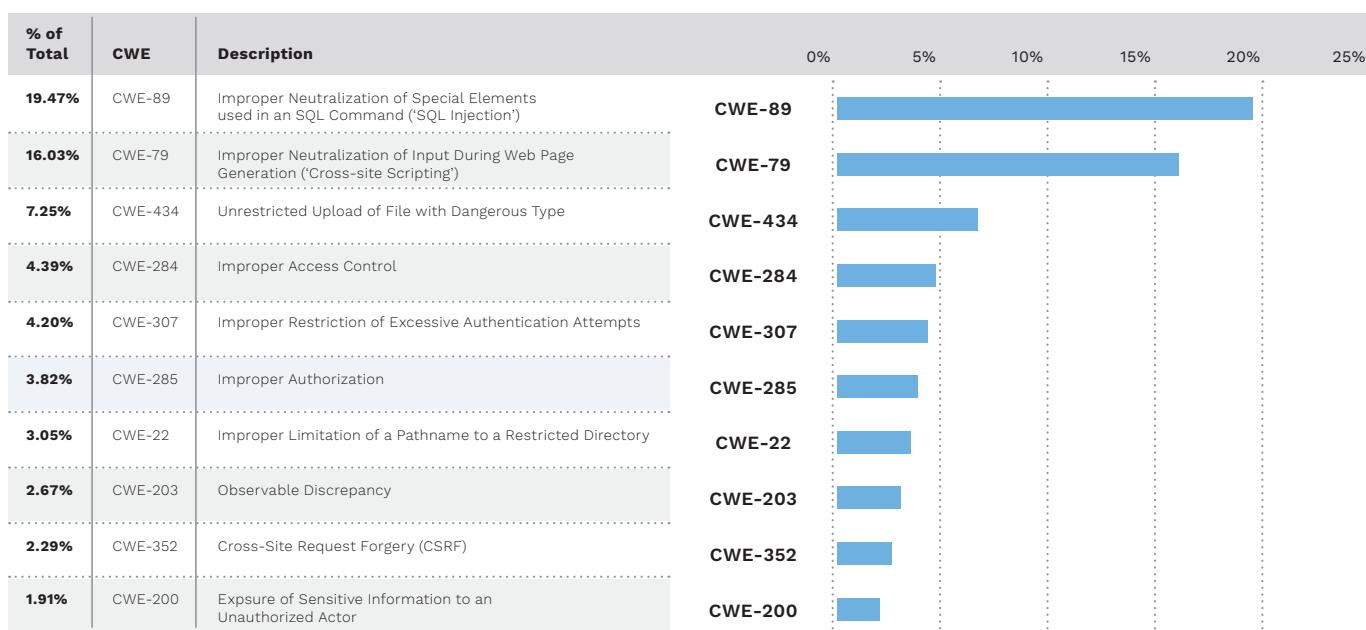
What is CWE?

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools and as a baseline for weakness identification, mitigation, and prevention efforts.

<https://cwe.mitre.org/>

CWE Dispersion - High & Critical Severity

IN TERMS OF CRITICAL SEVERITY WEB APPLICATION VULNERABILITIES, CWE-89 IS STILL THE MOST COMMON. THIS HAS NOT CHANGED SINCE 2022.



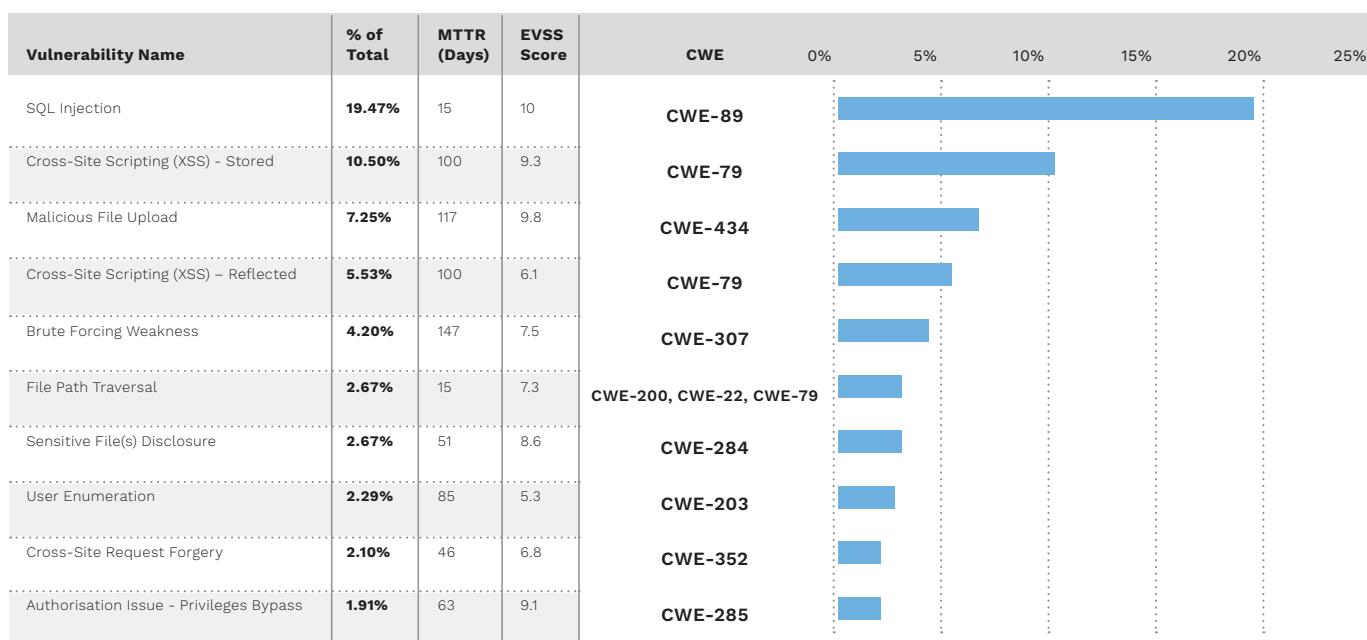
The SQL injection exploit was first documented in 1998 by cybersecurity researcher and hacker Jeff Forristal. His findings were published in the long running hacker zine Phrack.

Most Common High & Critical Severity Web Application Vulnerabilities

The Application Security Top 10 depicts the most common critical risk issues discovered by Edgescan over the past year. SQL Injection is still the main contender (as was in the 2023 report), which is interesting to note as we can easily develop code (or block vectors) to mitigate such attacks.

Detection of such vulnerabilities is also trivial using the correct techniques. Something which is overlooked quite frequently is “malicious file upload” at 7.25% of all High and Critical Severity vulnerabilities discovered. This can give rise to ransomware, malware and internal breach pivot points for attackers.

Web Application Vulnerabilities



% OF TOTAL

Percentage of total high and critical severity web application vulnerabilities discovered.

MTTR

MTTR (Mean time to remediate) is the speed at which we are fixing the discovered vulnerabilities. From discovery to fix and validation of fix.

EVSS SCORE

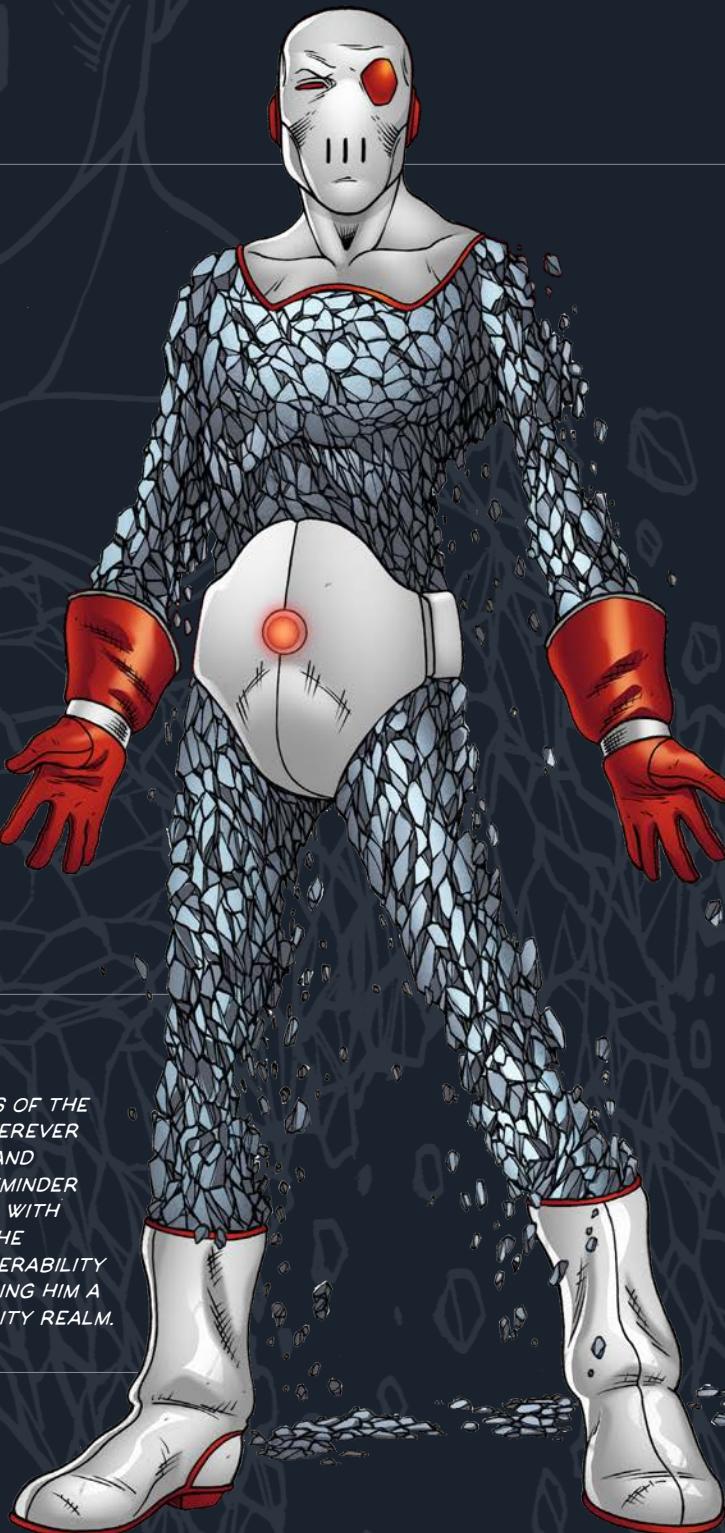
“Critical Severity” vulnerabilities are defined by the Edgescan Validated Security Score (EVSS) which is a combination of cyber analytics and expert validation.

INSIGHT FROM THIS REPORT...

The most common critical web application vulnerability is **SQL INJECTION (CWE-89)** – a vulnerability from 1998!

MR. VULNERABILITY

MR. VULNERABILITY THRIVES IN THE SHADOWS OF THE DIGITAL WORLD, EXPLOITING WEAKNESSES WHEREVER THEY LIE. AS THE ARCH-ENEMY OF SECURITY AND RESILIENCE, HIS PRESENCE IS A CONSTANT REMINDER OF THE BATTLE BETWEEN CHAOS AND ORDER. WITH A CUNNING MIND AND A KNACK FOR FINDING THE SLIGHTEST CRACK IN ANY DEFENSE, MR. VULNERABILITY CHALLENGES EDGESCAN AT EVERY TURN, MAKING HIM A FORMIDABLE ADVERSARY IN THE CYBERSECURITY REALM.



CISA KEV

As of January 2024, below is the list of vulnerabilities associated with each vendor according to the CISA KEV.

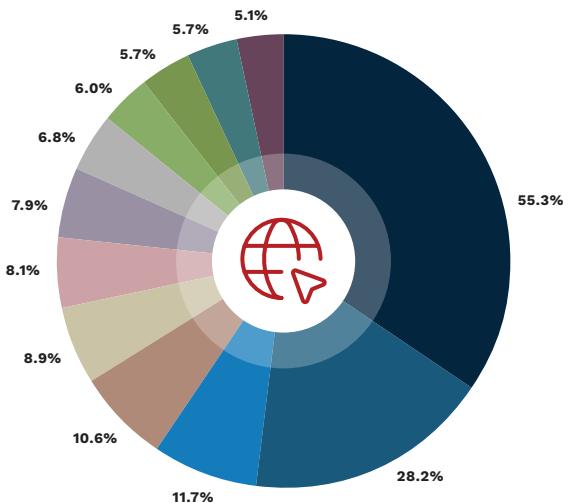
188 vulnerabilities were added in 2023.

CISA KEV VULNERABILITY DISPERSION BY VENDOR

 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

Most Common Vulnerability With EPSS >0.8

80% PROBABILITY OF BREACH – PUBLIC INTERNET FACING



Technology	% of Total	MTTR (Days)	CWE	CVE	CISA KEV	CVSS	EPSS	EXF	Exploit Code Exists
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (LogJam)	55.3%	65.4	CWE-310	CVE-2015-4000	FALSE	3.7	0.97493	82	
SSL/TLS: Weak Cipher Suites	28.2%	60.5	CWE-310, CWE-326, CWE-327	CVE-2013-2566, CVE-2015-2808, CVE-2015-4000	FALSE	5.9	0.97493	83	
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	11.7%	274.8	CWE-310	CVE-2014-3566	FALSE	3.4	0.97505	82	Yes
Microsoft Exchange Server 2013 / 2016 / 2019 Multiple Vulnerabilities	10.6%	152.9	CWE-290	CVE-2021-41349, CVE-2021-42305, CVE-2021-42321	TRUE	8.8	0.90677	98	Yes
Cisco Adaptive Security Appliance Software Web Services Interface Cross-Site Scripting Vulnerabilities	8.9%	32.8	CWE-79	CVE-2020-3580	TRUE	6.1	0.97048	98	Yes
OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	8.1%	62.9	CWE-326	CVE-2014-0224	FALSE	7.4	0.97404	84	
PHP - Multiple Vulnerabilities	7.9%	62.9	CWE-119, CWE-125, CWE-185, CWE-189, CWE-190, CWE-193, CWE-20, CWE-200, CWE-400, CWE-416	CVE-2015-0235, CVE-2022-31629, CVE-2014-9425, CVE-2014-9709, CVE-2015-1385, CVE-2015-1352, CVE-2015-8383, CVE-2015-8386, CVE-2015-8387, CVE-2015-8388, CVE-2015-8390, CVE-2015-8391, CVE-2015-8393, CVE-2015-8394, CVE-2015-8865, CVE-2016-10158, CVE-2016-21059, CVE-2016-21060, CVE-2016-21061, CVE-2016-3141, CVE-2016-3142, CVE-2016-40397, CVE-2016-40701, CVE-2016-4072, CVE-2016-4073, CVE-2016-4537, CVE-2016-4538, CVE-2016-4640, CVE-2016-4642, CVE-2016-5385, CVE-2016-5399, CVE-2016-6207, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6293, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297, CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128, CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132, CVE-2016-9935, CVE-2017-1142, CVE-2017-1143, CVE-2017-1144, CVE-2017-1145, CVE-2017-1146, CVE-2017-6004, CVE-2017-7890, CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, CVE-2017-9229	FALSE	9.8	0.95128	84	Yes
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	6.8%	274.8	CWE-310	CVE-2015-0204	FALSE	4.3	0.96454	82	
Wowza Streaming Engine – Multiple Log4j Vulnerabilities (Log4Shell)	6.0%	63.9	CWE-20, CWE-400, CWE-502, CWE-917	CVE-2021-44228, CVE-2021-45046	TRUE	10	0.97454	100	Yes
Apache Axis - Multiple Vulnerabilities	5.7%	32.5	CWE-79, CWE-918	CVE-2018-8032, CVE-2019-0227	FALSE	7.5	0.89205	83	
Apache HTTP Server – Multiple Vulnerabilities – Windows	5.7%	41.8	CWE-476, CWE-787, CWE-918	CVE-2021-34798, CVE-2021-39275, CVE-2021-40438	TRUE	9.8	0.97178	100	Yes
Cisco IOS XE Software Web UI Multiple Vulnerabilities	5.1%	115.5	CWE-269, CWE-250	CVE-2023-20198, CVE-2023-20273	TRUE	10	0.89074	99	Yes

MTTR

MTTR (Mean time to remediate) is the speed at which we are fixing the discovered vulnerabilities. From discovery to fix and validation of fix.

CISA KEV

CISA KEV depicts if the vulnerability is listed on the Known Exploit catalogue managed by the Cyber Security and Infrastructure Agency (CISA)

<https://www.cisa.gov/>

EPSS

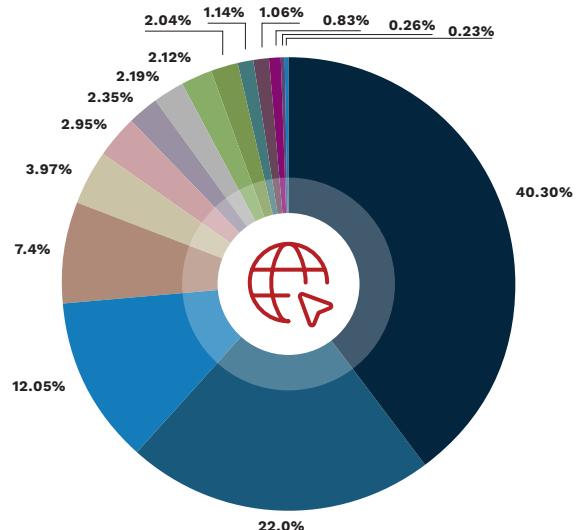
EPSS is the Exploit probability based on first.org data.

EXPLOIT CODE EXISTS

Exploit Code Exists signifies if exploit code is freely available on the public Internet.

Most Common Vulnerability With 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 Diffie-Hellman Modulus <= 1024 Bits (LogJam)	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-1284, 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-2021-3796, 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-2021-4069, CVE-2021-4136, CVE-2021-4166, CVE-2021-4192, CVE-2021-4193, CVE-2021-46059, CVE-2022-0128, CVE-2022-0213, CVE-2022-0261, CVE-2022-0318, CVE-2022-0319, CVE-2022-0351, CVE-2022-0359, CVE-2022-0361, CVE-2022-0392, CVE-2022-0407, 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-2022-1851, CVE-2022-1897, CVE-2022-1898, CVE-2022-1927, CVE-2022-1968, CVE-2022-2124, CVE-2022-2125, CVE-2022-2126, 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-2022-2257, CVE-2022-2264, CVE-2022-2284, CVE-2022-2285, CVE-2022-2286, CVE-2022-2287, CVE-2022-2304, CVE-2022-2343, CVE-2022-2344, CVE-2022-2345, CVE-2022-2522, CVE-2022-2571, CVE-2022-2580, CVE-2022-2581, CVE-2022-2598, CVE-2022-2816, CVE-2022-2817, CVE-2022-2819, CVE-2022-2845, CVE-2022-2849, CVE-2022-2862, CVE-2022-2874, CVE-2022-2889, CVE-2022-2923, CVE-2022-2946, CVE-2022-2980, CVE-2022-2982, CVE-2022-3016, CVE-2022-3037, CVE-2022-3099, 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-2022-3352, 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%	15.0	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-2020-1935, CVE-2020-1938, CVE-2018-11784, CVE-2012-0874, CVE-2013-4810	FALSE	7	0.8836	83	Yes

Most Common Vulnerability With 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
Oracle Java SE Multiple Vulnerabilities	2.19%	52.3	CWE-119, CWE-295, CWE-119, CWE-295	CVE-2019-2449, CVE-2014-0429, CVE-2014-0446, CVE-2014-0451, CVE-2014-0453, CVE-2014-0460, CVE-2014-2398, CVE-2014-2401, CVE-2014-2412, CVE-2014-2421, CVE-2014-2427, CVE-2013-2400, CVE-2013-2449, CVE-2013-2458, CVE-2013-2460, CVE-2013-2462, CVE-2013-3744, CVE-2013-1500, CVE-2013-1571, CVE-2013-2443, CVE-2013-2445, CVE-2013-2446, CVE-2013-2447, CVE-2013-2448, CVE-2013-2450, CVE-2013-2452, CVE-2013-2454, CVE-2013-2455, CVE-2013-2456, CVE-2013-2457, CVE-2013-2459, CVE-2013-2463, CVE-2013-2464, CVE-2013-2465, CVE-2013-2469, CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-0809, CVE-2013-1493, CVE-2012-1711, CVE-2012-1713, CVE-2012-1718, CVE-2012-1719, CVE-2012-1720, CVE-2012-1723, CVE-2012-1541, CVE-2012-3213, CVE-2012-3342, CVE-2013-0351, CVE-2013-0409, CVE-2013-0419, CVE-2013-0423, CVE-2013-0424, CVE-2013-0425, CVE-2013-0426, CVE-2013-0427, CVE-2013-0428, CVE-2013-0429, CVE-2013-0430, CVE-2013-0431, CVE-2013-0432, CVE-2013-0433, CVE-2013-0434, CVE-2013-0435, CVE-2013-0437, CVE-2013-0438, CVE-2013-0440, CVE-2013-0441, CVE-2013-0442, CVE-2013-0443, CVE-2013-0444, CVE-2013-0445, CVE-2013-0446, CVE-2013-0448, CVE-2013-0449, CVE-2013-0450, CVE-2013-1473, CVE-2013-1475, CVE-2013-1476, CVE-2013-1478, CVE-2013-1479, CVE-2013-1480, CVE-2013-1481, CVE-2013-1482, CVE-2012-0507, CVE-2011-3544, CVE-2011-3546, CVE-2011-3550, CVE-2011-3551, CVE-2011-3553, CVE-2011-3558, CVE-2011-3561, CVE-2009-3555, CVE-2010-0082, CVE-2010-0084, CVE-2010-0085, CVE-2010-0087, CVE-2010-0088, CVE-2010-0089, CVE-2010-0090, CVE-2010-0091, CVE-2010-0092, CVE-2010-0093, CVE-2010-0094, CVE-2010-0095, CVE-2010-0837, CVE-2010-0838, CVE-2010-0839, CVE-2010-0840, CVE-2010-0841, CVE-2010-0842, CVE-2010-0843, CVE-2010-0844, CVE-2010-0845, CVE-2010-0846, CVE-2010-0847, CVE-2010-0848, CVE-2010-0849	TRUE	10	0.94509	99	
Microsoft Message Queuing (MSMQ) RCE Vulnerability	2.12%	52.8		CVE-2023-21554	FALSE	10	0.96122	85	Yes
Sudo Heap-Based Buffer Overflow Vulnerability (Baron Samedit) - Active Check	2.04%	34.6	CWE-193	CVE-2021-3156, CVE-2012-0572, CVE-2012-0574, CVE-2012-1702, CVE-2012-1705, CVE-2012-4414, CVE-2012-5611, CVE-2013-0375, CVE-2013-0382, CVE-2013-0384, CVE-2013-0385, CVE-2013-0389, CVE-2012-0578, CVE-2012-5096, CVE-2012-5612, CVE-2013-0367, CVE-2013-0368, CVE-2013-0371, CVE-2013-0386, CVE-2017-3737, CVE-2018-2573, CVE-2018-2583, CVE-2018-2590, CVE-2018-2612, CVE-2018-2645, CVE-2018-2647, CVE-2018-2696, CVE-2018-2703, CVE-2015-3194, CVE-2016-0661, CVE-2016-0665, CVE-2016-0668, CVE-2017-3450, CVE-2017-3599, CVE-2015-3194	TRUE	7.8	0.96575	98	Yes
Missing Linux Kernel mitigations for 'Spectre variant 2' hardware vulnerabilities	1.14%	34.8	CWE-203	CVE-2017-5715	FALSE	5.6	0.97548	83	Yes
Apache HTTP Server - Multiple Vulnerabilities – Windows	1.06%	135.2	CWE-476, CWE-787, CWE-918	CVE-2012-0053, CVE-2021-34798, CVE-2021-39275, CVE-2021-40438, CVE-2013-1896, CVE-2019-10097	TRUE	9.8	0.97178	100	Yes
Elastic Elasticsearch Multiple Log4j Vulnerabilities (ESA-2021-31, Log4Shell)	0.83%	82.8	CWE-20, CWE-400, CWE-502, CWE-917	CVE-2021-44228, CVE-2021-45046	TRUE	10	0.97454	100	Yes
VMware ESXi Multiple Vulnerabilities	0.26%	66.5	CWE-119, CWE-20, CWE-415	CVE-2015-7547, CVE-2015-1047, CVE-2015-2342, CVE-2015-5177, CVE-2014-3513, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568, CVE-2014-3660, CVE-2014-8370, CVE-2015-1043, CVE-2015-1044, CVE-2010-5298, CVE-2014-0198, CVE-2014-0224, CVE-2014-3470, CVE-2013-0242, CVE-2013-1914, CVE-2013-4322, CVE-2013-4590, CVE-2014-0050, CVE-2014-0114	FALSE	7	0.97298	84	Yes
Oracle MySQL ServerMultiple Vulnerabilities	0.23%	77.7		CVE-2015-3194, CVE-2016-0661, CVE-2016-0665, CVE-2016-0668	FALSE	7.5	0.94433	83	

MTTR

MTTR (Mean time to remediate) is the speed at which we are fixing the discovered vulnerabilities. From discovery to fix and validation of fix.

CISA KEV

CISA KEV depicts if the vulnerability is listed on the Known Exploit catalogue managed by the Cyber Security and Infrastructure Agency (CISA)

<https://www.cisa.gov/>

EPSS

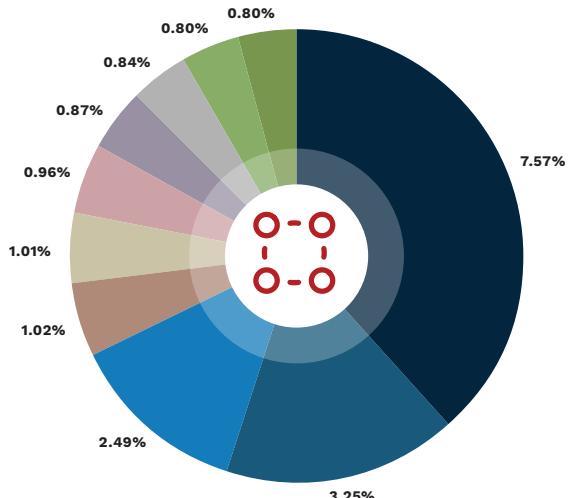
EPSS is the Exploit probability based on first.org data.

EXPLOIT CODE EXISTS

Exploit Code Exists signifies if exploit code is freely available on the public Internet.

Most Common High & Critical Severity (CVSS)

NON-INTERNET FACING NETWORK VULNERABILITIES



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-2015-4902, CVE-2015-4903, CVE-2015-4911	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-2021-4069, CVE-2021-4136, CVE-2021-4166, CVE-2021-4192, CVE-2021-4193, CVE-2021-46059, 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	
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 (RXR20J) (KRX22-002)(No Creds) (RCE) (RXR20I/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

MTTR

MTTR (Mean time to remediate) is the speed at which we are fixing the discovered vulnerabilities. From discovery to fix and validation of fix.

CISA KEV

CISA KEV depicts if the vulnerability is listed on the Known Exploit catalogue managed by the Cyber Security and Infrastructure Agency (CISA)

<https://www.cisa.gov/>

EPSS

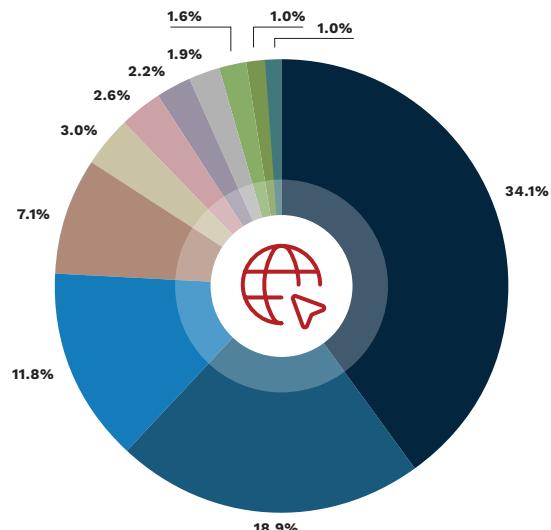
EPSS is the Exploit probability based on first.org data.

EXPLOIT CODE EXISTS

Exploit Code Exists signifies if exploit code is freely available on the public Internet.

Most Common High & Critical Severity (CVSS)

PUBLIC INTERNET EXPOSED VULNERABILITIES



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	
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-2021-22659, CVE-2017-16740, CVE-2015-6486, CVE-2015-6428, 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

MTTR (Mean time to remediate) is the speed at which we are fixing the discovered vulnerabilities. From discovery to fix and validation of fix.

CISA KEV

CISA KEV depicts if the vulnerability is listed on the Known Exploit catalogue managed by the Cyber Security and Infrastructure Agency (CISA)

<https://www.cisa.gov/>

EPSS

EPSS is the Exploit probability based on first.org data.

EXPLOIT CODE EXISTS

Exploit Code Exists signifies if exploit code is freely available on the public Internet.

INSIGHTS FROM THIS REPORT...

The mean time to remediate (MTTR) a critical severity web application vulnerability is **35 DAYS**.

Internet facing host/cloud critical severity vulnerability MTTR is **61 DAYS**.

MEET FALSE POSITIVE

MASTER OF DECEPTION, FALSE POSITIVE, WEAVES A COMPLEX WEB OF ILLUSIONS, LEADING EVEN THE MOST VIGILANT ASTRAY. HER ABILITY TO MIMIC GENUINE THREATS EXHAUSTS RESOURCES AND BURNS THROUGH PRECIOUS TIME WITH HER CONVINCING MASQUERADES. HER EXPERTISE IN SOWING CONFUSION MAKES HER AN EXPERT IN DERAILING THE FOCUS OF CYBERSECURITY TEAMS, MAKING HER A CRITICAL THREAT IN THE DIGITAL BATTLEFIELD.



FALSE POSITIVE SLOWS DOWN MEAN TIME TO REMEDIATION BY ENSURING YOU DON'T KNOW WHICH VULNERABILITIES ARE REAL.



FALSE POSITIVE CAN WREAK HAVOC, BUT VALIDATOR CAN DEFEAT HER QUICKLY BY ENSURING ALL OF YOUR VULNERABILITIES ARE REAL. IF YOU SEE FALSE POSITIVE LURKING IN THE SHADOWS MAKE SURE TO CALL VALIDATOR!

MTTR

Based on EPSS

—VS—

MTTR

Based on CVSS

It is currently unclear if vulnerabilities are closed quicker based on CVSS or EPSS scores. There is a loose correlation between EPSS and CVSS but it's not linear. Over the coming years looking at MTTR compared to EPSS and CVSS will indicate if EPSS is taking more traction in the industry.

EPSS	MTTR (Days)
>0.8	61.55
0.5 to 0.79	56.68
0.3 to 0.49	75.98
0.1 to 0.29	43.84
0.1 to >0.99	62.5

>0.8
61.55 DAYS

0.5 to 0.79
56.68 DAYS

0.3 to 0.49
75.98 DAYS

0.1 to 0.29
43.84 DAYS

0.1 to >0.99
62.5 DAYS

CVSS	MTTR (Days)
>9.0	45.46
7.5 to 8.9	55.56
6.0 to 7.4	59.92
3.0 to 5.9	61.33
1.0 to 2.9	50.32

>9.0
45.46 DAYS

7.5 to 8.9
55.56 DAYS

6.0 to 7.4
59.92 DAYS

3.0 to 5.9
61.33 DAYS

1.0 to 2.9
50.32 DAYS

MTTR

MTTR measures how quickly a vulnerability can be remediated and validated as such after it is first detected. It provides insights into the efficiency of remediation processes and the team's ability to bounce back from incidents. A lower MTTR indicates faster recovery and better system reliability.

MTTR

Web Application

MTTR

Host/Network

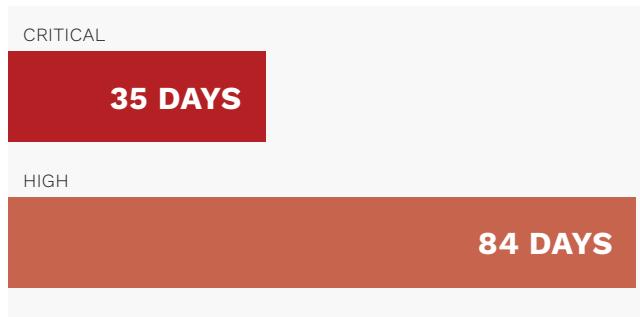
How quick are we addressing vulnerabilities based on severity in web applications?

Severity	CVSS V2.0 Ratings	CVSS V3.0 Ratings
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 Network/Host – Internet Facing



MTTR Web Applications

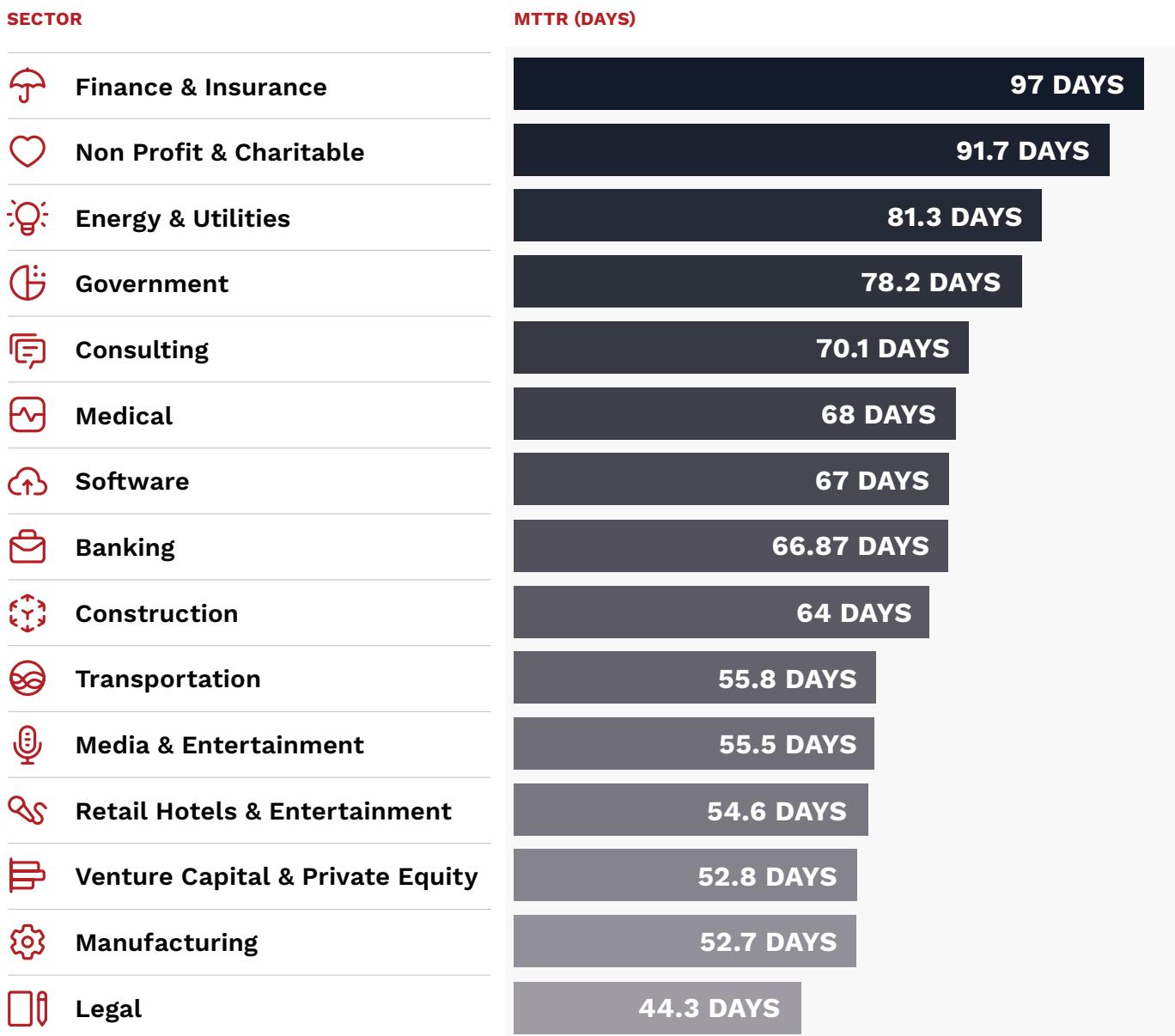


MTTR Network/Host – Non Internet Facing



MTTR Per Industry

In 2023, we examined fifteen different industries to report on their average rates of MTTR within that industry. We can see that the shortest MTTR can be seen in Legal at 44 days, while the longest is Finance & Insurance at 97 days.



INSIGHT FROM THIS REPORT...

YOU CAN'T SECURE WHAT YOU CAN'T SEE!

Attack Surface Management allows you to discover and monitor your assets continuously.

WHO IS MAPPER?

MAPPER STANDS AS A VIGILANT SENTINEL, HIS EYES SCANNING THE HORIZON FOR POTENTIAL THREATS. WITH AN UNPARALLELED ABILITY TO IDENTIFY THE ATTACK SURFACE, HE ENSURES THAT NO VULNERABILITY GOES UNNOTICED. HIS CONTINUOUS VIGILANCE IS A BEACON OF HOPE, GUIDING THE FORCES OF GOOD IN THEIR UNENDING QUEST TO PROTECT THE DIGITAL REALM.



Most Common Network/Host Vulnerability

PER INDUSTRY CVSS >7.0

Industry	Vulnerability	CVE	CVSS	EPSS	Exploit Code Available
 Media & Entertainment	Wowza Streaming Engine – Multiple Log4j Vulnerabilities (Log4Shell)	CVE-2021-44228, CVE-2021-45046	10	0.97454	
 Legal	Microsoft Message Queuing (MSMQ) – RCE Vulnerability	CVE-2023-21554	10	0.96122	
 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	
 Retail Hotels & Entertainment	VNC Brute Force Login	-	9	-	
 Venture Capital & Private Equity	Microsoft Exchange Server OWA – Multiple Vulnerabilities	CVE-2022-41040, VE-2022-41082	8.8	0.96949	Yes
 Manufacturing	SUSE: Security Advisory (SUSE-SU-2022:4240-1)	CVE-2022-43995	8.8	0.0045	
 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	
 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

Most Common Application Vulnerability

PER INDUSTRY > MEDIUM SEVERITY

Industry	Vulnerability	CWE	CVSS
 Media & Entertainment	SQL Injection	CWE-89	10
 Legal	Information Disclosure - Sensitive Information in URL	CWE-200	7.1
 Finance & Insurance	Cross-Site Request Forgery	CWE-352	6.8
 Retail Hotels & Entertainment	Sensitive Data Enumeration	CWE-204	9
 Venture Capital & Private Equity	Cross-Site Scripting (XSS) – Reflected	CWE-79	6.1
 Manufacturing	Cross-Site Scripting (XSS) - Stored	CWE-79	9.3
 Non Profit & Charitable	Sensitive File(s) Disclosure	CWE-200	8.6
 Government	XML External Entity Injection	CWE-611	7.7
 Medical	SQL Injection	CWE-89	10
 Consulting	Malicious File Upload	CWE-434	9.8
 Construction	SQL Injection	CWE-89	10
 Banking	Cross-site Request Forgery	CWE-352	6.8
 Energy & Utilities	Cross-Site Scripting (XSS) – Reflected	CWE-79	6.1
 Software	SQL Injection	CWE-89	10
 Transportation	SQL Injection	CWE-89	10

SQL INJECTION

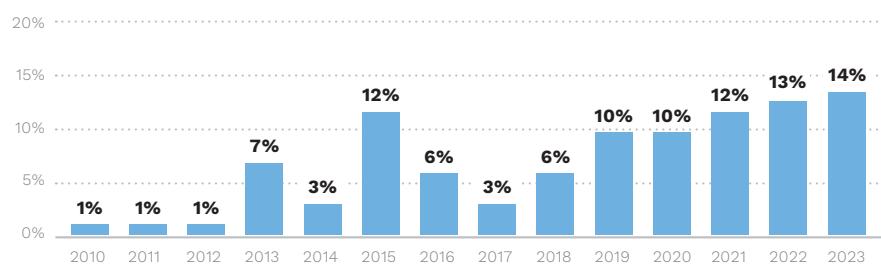
SQL Injection is a potentially devastating vulnerability and is the most common high & critical severity vulnerability in the media, medical, construction, software and transportation industries.

CROSS-SITE SCRIPTING

Cross-Site Scripting is common, albeit most modern browsers provide a level of protection against such weakness with technologies such as CSP (Content security policy).

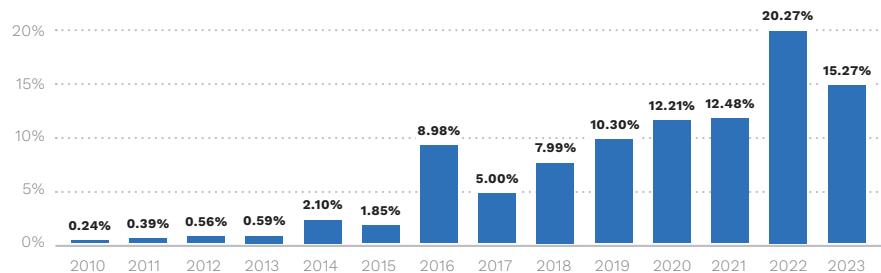
Vulnerabilities Discovered By Age

Vulnerabilities Discovered by Age



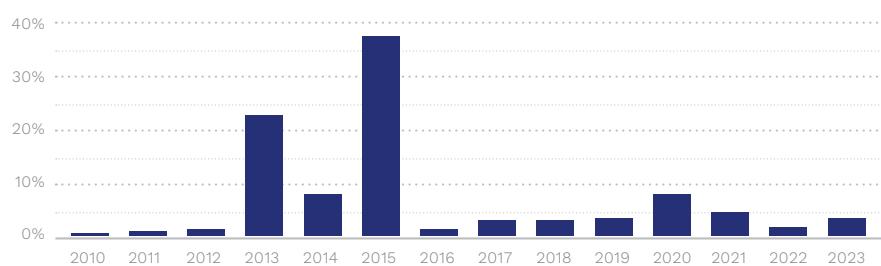
45% OF VULNERABILITIES DISCOVERED WERE BETWEEN 1 AND 4 YEARS OLD. THIS METRIC MAY SEEM POOR WHEN SEVERITY OR CVSS SCORE IS NOT CONSIDERED

Vulnerabilities >CVSS 7.0 by Age



WHEN WE LOOK AT VULNERABILITIES BY AGE FOR VULNERABILITIES WITH A CVSS >7.0 WE SEE **55%** ARE BETWEEN 1 AND 4 YEARS OLD

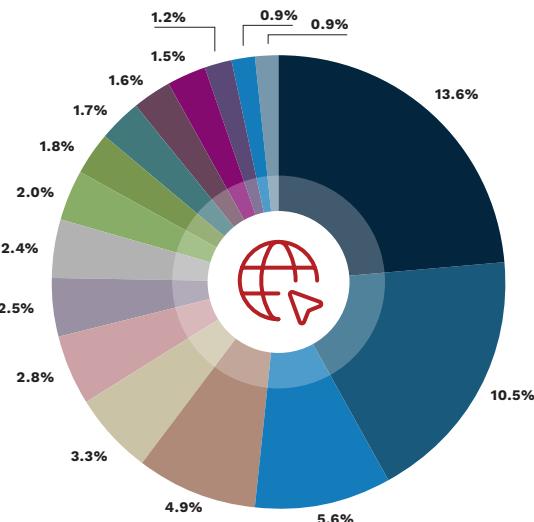
Vulnerabilities <EPSS 0.7 by Age



SPIKE IN **2015** IS DUE TO CRYPTO CVE'S WHICH HAVE A EPSS > 0.7, OF WHICH THERE ARE MANY

Attack Surface Management (ASM)

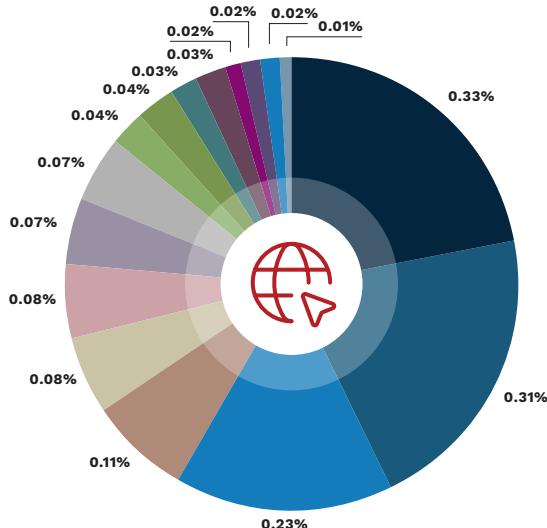
**BASED ON A SAMPLE OF 2,000,000
ENDPOINT SCANS THE BELOW DESCRIBES
EXPOSED PORTS, THEIR RATE OF OCCURRENCE
AND THE REASON NOT TO EXPOSE TO THE
PUBLIC INTERNET IF POSSIBLE**



Port	Protocol	Count	% Occurrence	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
554	tcp	8520	0.9%	Real Time Streaming Protocol (RTSP)	There are 141 CVE's related to this protocol

Attack Surface Management (ASM) – Bad Ports!

**BASED ON A SAMPLE OF 2,000,000 ENDPOINT SCANS
THE BELOW DESCRIBES EXPOSED PORTS, THEIR RATE OF OCCURRENCE AND THE REASON NOT TO EXPOSE TO THE PUBLIC INTERNET IF POSSIBLE**

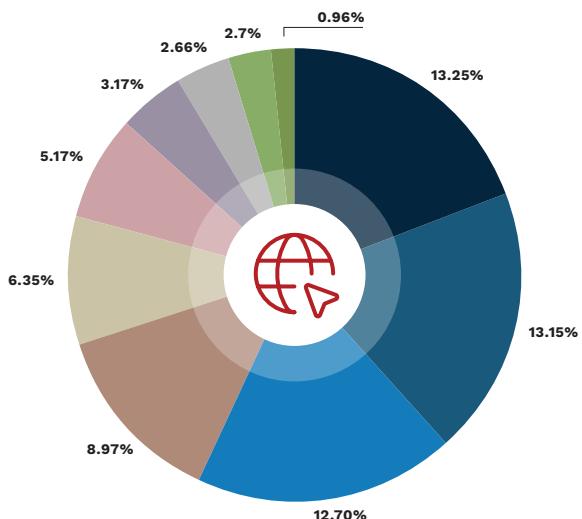


Port	Protocol	Count	% Occurrence	Description	Notes
7000	tcp	3240	0.33%	Exposed Cassandra Database Port	Exposed Database ports are trouble!
21	tcp	3040	0.31%	Ports 20 and 21: These are TCP-only ports used for FTP (File Transfer Protocol).	FTP is outdated and insecure, making these ports susceptible to 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.
6666	tcp	360	0.04%	Port 6666 and 6667 (IRC): Commonly used for Internet Relay Chat services.	Internet Relay Chat (IRC) ports are often used for botnets and malware control. If you're not running an IRC server, close these ports.
7001	tcp	320	0.03%	Exposed Cassandra Database Port	Exposed Database ports are trouble!
389	tcp	280	0.03%	TCP port 389 (and optionally TCP port 636) is used for LDAP.	If you need to expose LDAP externally, consider using VPN tunnels or other secure methods to connect to your internal network.
1521	tcp	240	0.02%	Exposed Oracle Database Port	Exposed Database ports are trouble!
1434	tcp	240	0.02%	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.
6667	tcp	160	0.02%	Port 6666 and 6667 (IRC): Commonly used for Internet Relay Chat services.	Internet Relay Chat (IRC) ports are often used for botnets and malware control. If you're not running an IRC server, close these ports.
9200	tcp	120	0.01%	Exposed Elasticsearch Database	Exposed Database ports are trouble!

% OF TOTAL

The relative percentages are small but such ports should not be exposed to the public Internet.

Risk Accepted Vulnerabilities



MOST COMMON VULNERABILITIES THAT ARE MARKED AS 'RISK ACCEPTED' IN THE EDGESCAN PLATFORM BY ORGANIZATIONS THEMSELVES

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

It appears closure of web application and API vulnerabilities is more consistent, given the majority of high and critical severity vulnerabilities in a vulnerability backlog (on average), reside in the network/host/device layer.

% OF TOTAL

% of Total is the percentage of all critical & High severity public Vulns discovered in 2023.

CISA KEV

CISA KEV signifies if at least one CVE is listed on the CISA KEV.

EPSS

EPSS is The Exploit Prediction Security Score at the time of writing. For multiple vulnerabilities it's the highest value.

Vulnerability Backlog

Vulnerability Backlog is the % of unclosed vulnerabilities an organization has within a 12 month period. This is typical of all organizations and most professionals agree that fixing all vulnerabilities is not a wise use of resources – fix what matters.

14.2%

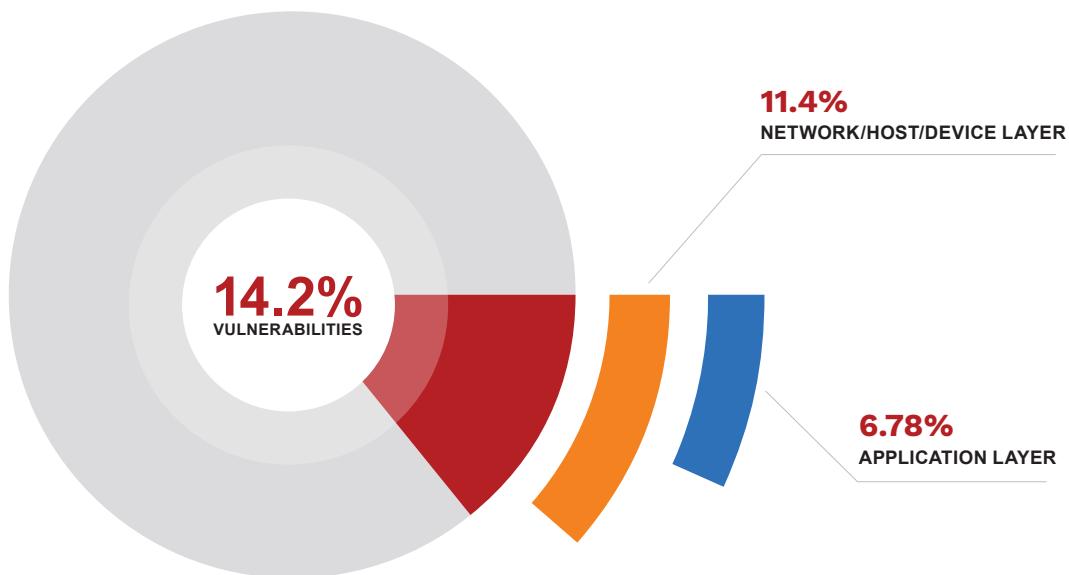
OF VULNERABILITIES IN AN ENTERPRISE'S BACKLOG ARE EITHER HIGH OR CRITICAL SEVERITY

11.4%

OF WHICH ARE ATTRIBUTED TO THE NETWORK/HOST/DEVICE LAYER

6.78%

OF WHICH ARE IN THE APPLICATION LAYER



For larger enterprises (1000+ employees), on average, 48% of vulnerabilities discovered in a 12 month period remain open – they have not been remediated.

It appears closure of web application and API vulnerabilities is more consistent, given the majority of high and critical severity vulnerabilities on average in a vulnerability backlog reside in the network/host/device layer.

Vulnerability Clustering

**METRICS RELATING TO THE AVERAGE AMOUNT OF VULNERABILITIES PER ASSET.
MOST ASSETS ACROSS THE FULL STACK HAVE MULTIPLE VULNERABILITIES.**

3.42%

OF ALL ASSETS HAVE AT LEAST 1 VULNERABILITY WITH AN EPSS SCORE >0.7

1.72%

OF ALL ASSETS HAVE AT LEAST 10 VULNERABILITIES WITH AN EPSS SCORE >0.7

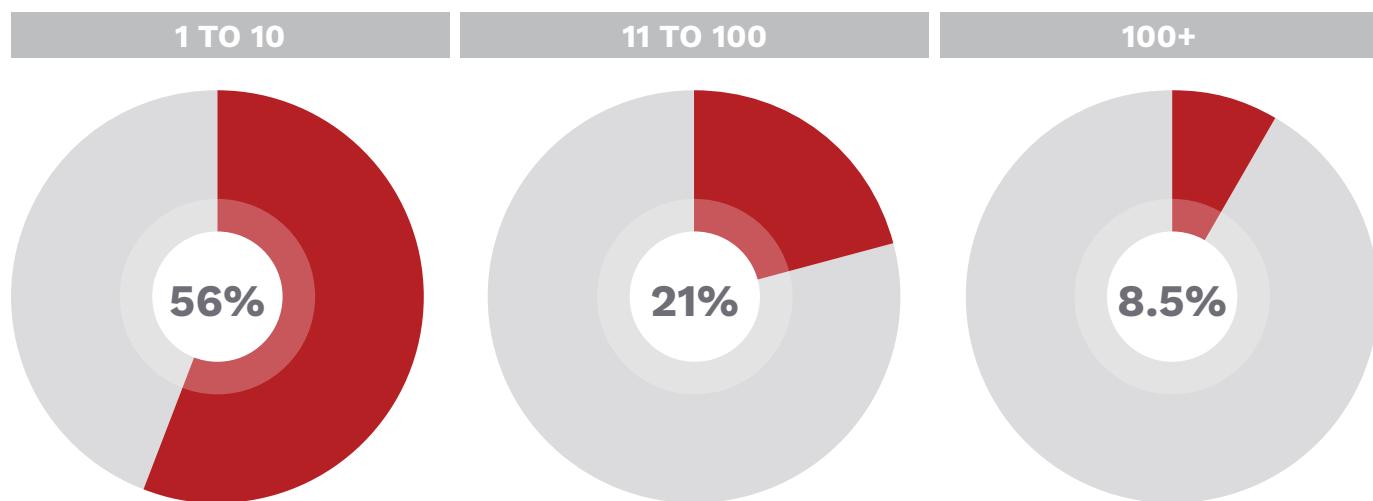
3/100

ASSETS HAVE A VULNERABILITY WITH A PROBABILITY OF BREACH ABOVE 70%

2/100

ASSETS HAVE 10+ VULNERABILITIES WITH A PROBABILITY OF BREACH AT LEAST 70%

Vulnerability Count



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

ASSETS

Assets are defined in Edgescan as an endpoint, API or Web Application.

Conclusion

WE ARE STILL NOT GETTING THE BASICS RIGHT

In 2023 we've observed very basic vulnerabilities many of which are commonly leveraged by cybercrime. Albeit easy to discover and validate they still persisted for up to 90 days on systems maintained by professional and skilled cyber security teams.

The challenge was visibility. Once the vulnerabilities were discovered they were mitigated quickly. Visibility is a cornerstone of cyber security coupled with continuous assessment and detection.

The one-off penetration test is dead. It does not keep pace with the rate of vulnerabilities in software and leaves an organizations window of exposure too large to deliver meaningful defense.

Continuous assessment, validation & prioritization will make a huge difference to any organizations cybersecurity posture. Combining metadata in relation to EPSS, CVSS, CISA KEV and if exploitable code is freely available makes for superior and rapid vulnerability management.

Resilience; Internal (Non-Internet Facing) Vulnerability Management is certainly overlooked, possibly the reason for the ease of pivot by cyber crime organizations once they breach the perimeter.

ASM, RBVM and PTaaS are all a combined means to a singular end. Think of it as visibility, surface scanning and deep testing. All are required even for organizations who have adopted a Shift-Left approach.

Attack Surface Management (ASM) is not a "Wishlist" item and aids decent vulnerability management coverage.

Many exposures detected by ASM, are not CVE/OWASP related but rather exposed services due to poor visibility.

Reliance on Shift-Left Security alone will not prevent the problem of system insecurity, i.e. looking at business system risk from a "Full Stack" perspective.

Remediation times need to come down. This may be due to poor prioritization and lack of understanding of "what matters" when assessing a "Vulnerability Backlog".

CISA KEV and EPSS are great tools when combined with CVSS. Validated, accurate vulnerability data has also proven to increase the speed of MTTR & manage vulnerability backlogs.

ASM

Attack Surface Management

RBVM

Risk-Based Vulnerability Management

PTAAS

Penetration Testing as a Service

What Is Edgescan

WHAT MAKES US TICK

Verified vulnerability intelligence

Real data. Actionable results.

During an assessment, the Edgescan validation engine queries millions of vulnerability examples stored in our data lake; our data is sourced from thousands of security assessments and penetration tests performed on millions of assets utilizing the Edgescan Platform. Vulnerability data is then run through our proprietary analytics models to determine if the vulnerability is a true positive. If it meets a certain numeric threshold it is released to the customer; we call this an auto-commit vulnerability.

If the confidence level falls below the threshold, the vulnerability is flagged for expert validation by an Edgescan security analyst. This hybrid process of automation and combined human intelligence is what differentiates us from scanning tools and legacy services providing real and actionable results.

Accurate data

Really accurate data.

Since 2015 Edgescan has annually produced the Vulnerability Statistics Report to provide a global snapshot of the overall state of cybersecurity using intelligence obtained from the Edgescan data lake.

This yearly report has become a reliable source for approximating the global state of vulnerability management and enterprises security postures. This is exemplified by our unique dataset being part of the Verizon Data Breach Report (DBIR), which is the de facto standard for insights into the common drivers for incidents and breaches today.

Happy customers

95% renewal rate.

Edgescan is a true white glove service that eliminates the need for tool configuration, deployment, and management. By providing vulnerability intelligence and remediation information along with human guidance and vulnerability verification, we help our customers prevent security breaches, safeguarding their data and IT assets.

Customer satisfaction is seen in our retention rate of 95% and the amazing product reviews on Gartner Peer Insights and G2, as well as our stellar customer testimonials.

"The accuracy that comes with human validation, paired with the efficiency of automatic, continuous scanning, means that my team now knows that whenever a vulnerability is flagged, the vulnerability is there, and they can continue working until they find it and fix it."

Archroma Life Enhanced



Edgescan Reviews

 Customer First

by Edgescan in Application Security Testing

4.7 ★★★★ 44 Ratings

The Risk-Based Vulnerability Management Platform

ONE PLATFORM FOR COMPLETE RISK-BASED VULNERABILITY MANAGEMENT

Comprehensive visibility into your cyber footprint via Risk-Based Vulnerability Management, External Attack Surface Management, and Penetration Testing as a Service.

Discover and continuously monitor your organization's attack surface, perform automated network vulnerability scanning and DAST on-demand, on a schedule, or continuously. All automated assessment results are 100% validated findings and include expert remediation guidance. Edgescan's certified security experts provide consultancy-grade penetration testing of your most critical assets, with all findings delivered to the platform, unlimited retesting of findings, and reporting on-demand.

Unite best-in-class testing across networks, APIs, web applications, and mobile applications to clearly understand and track your risk posture. Contextualize your organization's risk with validated vulnerability intelligence, traditional scoring and reference systems, and Edgescan's proprietary risk rating systems to prioritize the most important vulnerabilities first.

Full-stack coverage and a hybrid approach ensure you can have a true understanding of your attack surface, and the vulnerabilities within. Edgescan gives your team everything they need to maintain a proactive and robust risk-based vulnerability management program.



Key features and benefits:

Hybrid approach

Automated vulnerability assessments, validated vulnerability intelligence, consultancy-grade penetration testing

Unlimited automated scanning

For network infrastructure, APIs, and web applications

Validated vulnerabilities

100% verified, falsepositive free

Consultancy-grade penetration testing

Delivered as a service by certified security experts

Risk-based vulnerability intelligence

Contextualized risk through traditional and proprietary systems

Unlimited retesting

Retest any vulnerability, anytime

Expert remediation guidance and support

Direct access to certified pen testers

Core Edgescan Products



Edgescan Penetration Testing as a Service (PTaaS)

Consultancy-grade network penetration test, API, mobile or web application business logic assessment performed by Edgescan's team of certified security experts. All results delivered via the Edgescan RBVM Platform include unlimited retesting of all findings. Includes automated scanning of target asset(s) (i.e. Edgescan NVS, Edgescan DAST, Edgescan DAST for APIs).



Edgescan Dynamic Application Security Testing (DAST)

Automated DAST for web applications, with a 100% validated result. Includes Edgescan NVS for the underlying host(s).



Edgescan DAST for APIs

Automated DAST for APIs, with a 100% validated result. Includes Edgescan NVS for the underlying host(s).



Edgescan Network Vulnerability Scanning (NVS)

Automated vulnerability scanning for layer 2 and 3 network infrastructure, peripherals, and workstations, with a 100% validated result.



Edgescan Mobile Application Security Testing (MAST)

A combination of a native device penetration testing and forensic analysis of a mobile application, as well as business logic assessment of the underlying API for the mobile OS (iOS or Android), performed by Edgescan's team of industry certified security experts. All results delivered via the Edgescan RBVM Platform include unlimited retesting of all findings. Includes Edgescan DAST for APIs on the mobile application's underlying API.

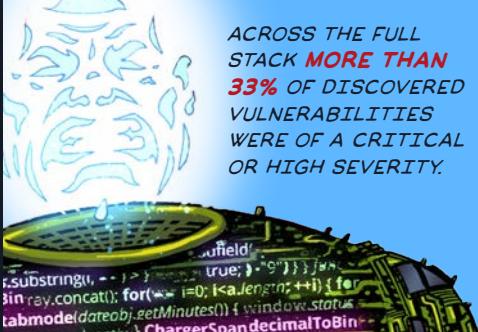


Edgescan External Attack Surface Management (EASM)

Provides visibility of an enterprise's internet-facing assets. Seamlessly identify assets requiring more comprehensive vulnerability assessment and transition them to an appropriate level of vulnerability testing. Continuously monitor your attack surface for shadow IT, rogue APIs, and alert on changes.



WELCOME TO THE EDGESCAN UNIVERSE



ACROSS THE FULL
STACK **MORE THAN**
33% OF DISCOVERED
VULNERABILITIES
WERE OF A CRITICAL
OR HIGH SEVERITY.



188
VULNERABILITIES
WERE ADDED IN
2023 TO THE
CISA KEV
IN 2023.



LEARN MORE ABOUT THE EDGESCAN HEROES, DEFENDERS OF CYBER SECURITY,
AND THE VILLAINS AND INFOSEC CHALLENGES THEY FACE AT [EDGESCAN.COM](https://edgescan.com)