

2023 Vulnerability Statistics Report

8th Edition



Table of Contents

Introduction	03
2022 Year in Review	04
Report Synopsys	06
Risk Density	08
Web Applications - Critical Severity Vulnerabilities	09
Web Applications - High Severity Vulnerabilities	10
Web Applications - Medium Severity Vulnerabilities	11
API - Critical and High Severity Vulnerabilities	12
Vulnerability Severity - EPSS, CISA KEV, and EVSS	14
Internet Facing Vulnerabilities - Critical Severity	15
Internet Facing Vulnerabilities - High Severity	16
Non-Internet Facing Vulnerabilities - Critical Severity	17
Non-Internet Facing Vulnerabilities - High Severity	19
Most Common Vulnerabilities listed on the CISA KEV	20
Highest Probability of Exploitation (EPSS) Internet Facing	21
Highest Probability of Exploitation (EPSS) Non-Internet Facing	22
Attack Surface Management (ASM) - Exposure Landscape	23
Mean Time to Remediate (MTTR) Time it takes to fix Vulnerabilities across the Full Stack	25
MTTR by Industry - Mean Time to Remediate Vulnerabilities	26
Risk Accepted	27
CISA KEV	29
Vulnerability Age	31
Vulnerability Clustering	32
Vulnerability Backlog	33
Conclusions	34
Why Edgescan - What makes us tick	35
Glossary	39

Introduction

Welcome to the 8th edition of the Edgescan Vulnerability Stats Report 2023. 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 2022.

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 organisations 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 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're 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 for four tiers of business sizes based on employee count and a distinction between internet facing and internally facing assets.

We take a look at how quickly various vulnerabilities are being fixed based on risk. 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.

New in this report is the way we look at prioritization and risk scores. Since Edgescan employs a number of risk prioritization scoring mechanisms, we take a deeper look at the most common risks faced by organisations 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 ¹CVSS (Common Vulnerability Scoring System), ²CISA KEV (Cyber Security & Infrastructure Security Agency Known Exploited Vulnerability Catalogue), ³EPSS ([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 faced by systems deployed in modern enterprises are.

¹ www.first.org/cvss/

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

³ www.first.org/epss/



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 2022 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



**“WE CAN'T IMPROVE WHAT
WE CAN'T MEASURE;
WE CAN'T SECURE WHAT
WE CAN'T SEE”**



“

**Fear cuts
deeper than
swords”**

George R.R. Martin,
A Game of Thrones

Report Synopsys

Non-internet facing systems have a significant risk density

- Our data indicates internal systems are less hardened than Internet facing systems (which is no surprise) and many feature prominently exploitable applications like Mozilla Firefox and Adobe with multiple CVE's that are listed on the CISA KEV. For example, The Adobe vulnerabilities commonly found are listed on the CISA KEV and have an EPSS score of 86%.
- This “target rich environment” allows threat actors to easily pivot within a local network post initial-access (breach) at the perimeter.
- So called, “Shift-Left” security is not taking into account the live environment on which systems are deployed, resulting in undetected weaknesses in the overall network of systems. Systems being assessed in a “lab” environment are not reflective of the risks when deployed on the public Internet.

Mean Time To Remediation (MTTR) for Critical Severity vulnerabilities is 65 days (across the full stack).

And while this result is similar to previous years, industry reports estimate that adversaries are now able to exploit a vulnerability within 15 days (on average) of discovery¹.

One third of all vulnerabilities across the full stack discovered in 2022 were either High or Critical Severity.

- While credential theft and stuffing is the most common mechanism for exploitation and phishing is second, exploiting vulnerabilities is the third most common vector to breach an organisation (according to the Verizon DBIR). CISA recommends fixing critical severity vulnerabilities within 15 days and high severity vulnerabilities within 30 days. Both secure development and continuous monitoring needs improvement, given that many of the high and critical severity issues seen in live environments are trivial to remediate.

The most common application layer vulnerabilities are still injection related, this also applies to API's.

- We are still seeing vulnerabilities which are not particularly new or exotic, but are widespread and very effective in terms of successful breach. Many injection related vulnerabilities can be easily detected using automation if applied on a frequent basis and importantly, if assessment coverage can be assured.

CISA KEV & EPSS combined are very useful in moving towards Risk Based Vulnerability Management (RBVM).

- Our report notes instances when EPSS and CISA

KEV do not align. CVSS score alone does not provide adequate metadata to help make risk based decisions. A combination of CVSS, EPSS, CISA KEV, and security validation is required to deliver risk based prioritization².

Prioritization needs to take into account the criticality of the asset.

- Given limited resources, proper prioritization is key to success as noted in the report. Additionally asset criticality must be a factor in the prioritization calculus. Understanding which assets are business critical and combining that information with vulnerability scoring information, is an indicated path to achieving true Risk Based Vulnerability Management.

Convergence of Vulnerability Management and Penetration Testing output is highly effective.

- Cybersecurity is perhaps more of a qualitative than quantitative effort. When identifying vulnerabilities in systems it is necessary to prioritize risks. However, prioritization alone is not sufficient, as we see when we layer in exploitability metrics with EPSS and EVSS, or when we also take into account asset value. Another level of validation needs to occur (like quality assurance of software releases) and that is essentially what penetration testing provides. Penetration testing is the qualitative proof, for security controls or exploitable vulnerabilities that should be remediated immediately.
- Combining intelligence harvested from both manual penetration testing (for depth) and vulnerability scanning (for frequency) – different means to the same end – can significantly help with prioritization and identification of risks.

Oddly, many “PCI Fails” are essentially “false flags” not listed on the CISA KEV or having a high EPSS probability score.

- A PCI compliance failure may occur because a CVE has a CVSS score above 4.0, without having any known exploits in the wild or impact on real world security via penetration test validation.
- This leads us to conclude that *Compliance and Security are certainly not the same*. And unfortunately, compliance may be creating more harm than good by distracting from the real work of RBVM.

1- https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdf

2- <https://www.cisa.gov/known-exploited-vulnerabilities> <https://www.first.org/epss/> <https://nvd.nist.gov/vuln-metrics/cvss>

“

**Those who
ignore Statistics
are condemned
to reinvent it**

Bradley Efron

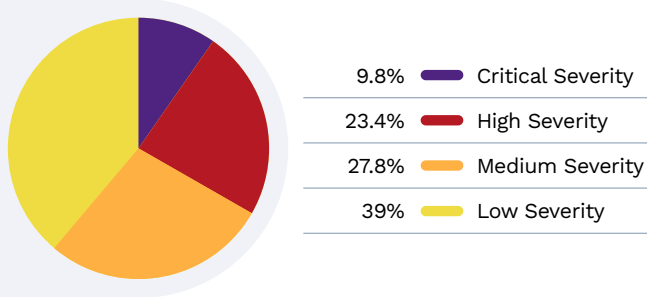
Risk Density

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.

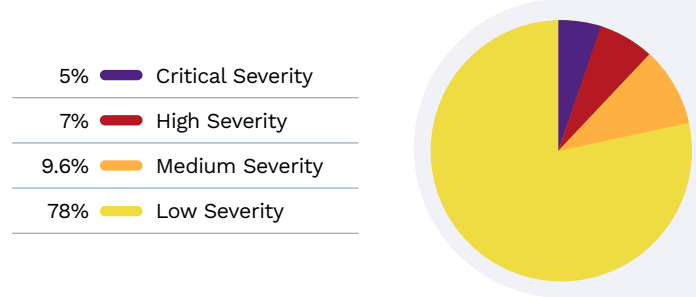
Severity is defined via the Edgescan Validated Security Score (EVSS). Later in the report we draw upon CVSS, CISA KEV and EPSS Risk and Probability scores.

Full stack



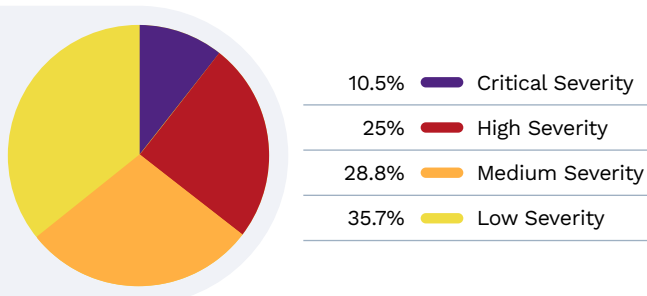
Across the full stack more than 33% of discovered vulnerabilities were of a critical or high severity.

Application



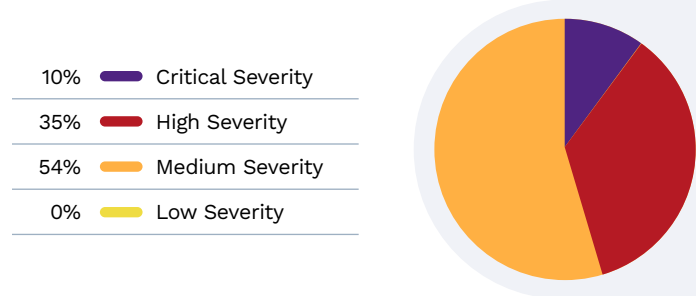
Across the Web application and API layers 12% of discovered vulnerabilities were of a critical or high severity.

Network



35.5% of discovered vulnerabilities in the infrastructure/hosting/cloud/network layer were of a critical or high severity.

PCI Failures



54% of PCI failures were of medium Severity. *Research indicates that such vulnerabilities will never be exploited, albeit they result in a PCI DSS compliance fail.*

Web Applications

Critical Severity Vulnerabilities

The Application Security Critical severity 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 2022 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 22.7% of all critical vulnerabilities discovered. This can give rise to ransomware, malware and internal network

breach pivot points for attackers.

Log4Shell (First discovered in late 2022) contributed to 5% of all critical severity vulnerabilities discovered this year.

Authorization issues cover privilege escalation or access to restricted functionality which would result in a data breach.

The most commonly found critical severity vulnerabilities across the application/web layer. “Critical Severity” vulnerabilities are defined by the Edgescan Validated Security Score (EVSS) which is a combination of analytics and expert validation.

23.4% CWE-89
SQL injection On CISA KEV **Yes**

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query. Various attacks can be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and executing operating system commands.

22.7% CWE-434
Malicious File Upload

Uploaded viruses and malware could later be downloaded by users of the application. Such malware can cause partial or complete compromise of a network that the host resides on.

19.1% CWE-79
Cross-Site Scripting (Stored)

Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent or Type-II XSS.

7.8% CWE-285
Authorization Issue - Privilege Bypass

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the users limits.

7.1% CWE-264
PHP Multiple Vulnerabilities

CVE-2012-2688,CVE-2012-3365

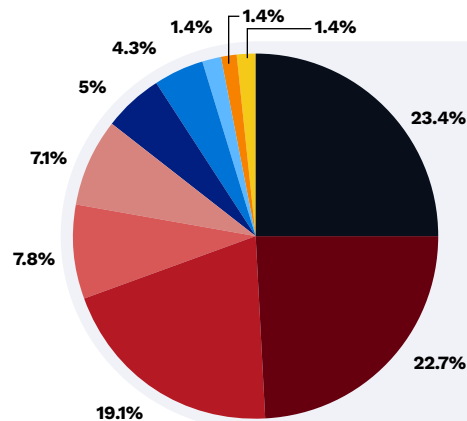
Multiple vulnerabilities pertaining to PHP patching.

5% CWE-917
Log4Shell (CVE-2021-44228)

CVE-2021-44228

On CISA KEV **Yes**

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can exploit this, via a web request to execute arbitrary code with the permission level of the running Java process.



4.3% CWE-94
Spring4Shell

CVE-2022-22965

On CISA KEV **Yes**

This is a remote code execution (RCE) vulnerability via data binding.

1.4% CWE-521
Weak Password Policy

Poor password controls such as no MFA, Default Credentials etc.

1.4% CWE-200
Database Console Exposure

The Database console was accessible, and provides access to privileged functionality which should not be accessible, except by authorized users or networks. Access to the console could allow a malicious actor to execute SQL statements on the sever.

1.4% CWE-35
File path traversal

CVE-2012-2688,CVE-2012-3365

This allows attackers to traverse the file system to access files or directories that are outside of the restricted directory.

Web Applications

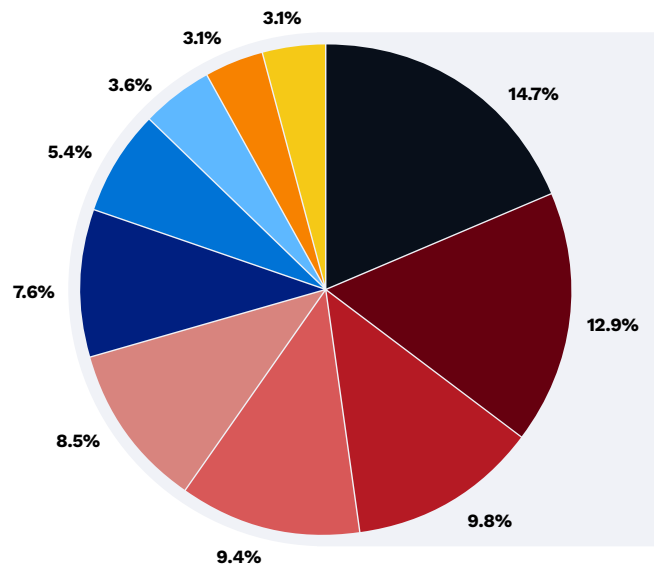
High Severity Vulnerabilities

Broken Authentication/Brute forcing possible (14.7%) is high on the list for 2022. This relates to misconfigured, broken logic, username enumeration or insecure authentication functionality.

Deserialization of Untrusted Data has also increased since 2021 (3.2%) to 9.4%.

As ever Cross-Site Scripting - XSS (Reflected) at 12.9% is a common vulnerability. Many browsers are getting better at protecting against such an attack vector, but not infallible.

The most commonly found high severity vulnerabilities across the application/web layer. "High Severity" vulnerabilities are defined by the Edgescan Validated Security Score (EVSS) which is a combination of analytics and expert validation.



14.7% CWE-307

Broken Authentication/Brute Forcing/User enumeration

Authentication in the application did not function correctly or it was possible to perform a brute forcing attack on the users of this web application. A common attack by malicious users is to attempt a number of different combinations of passwords, IDs or 2FA codes in order to gain unauthorized access to an account or user data.

12.9% CWE-79, CWE-725

Cross-Site Scripting - XSS (reflected)

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request which, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that users session with the application.

9.8% CWE-643, CWE-91

XML External Entity Injection (XXE)

XML injection which resulted in application compromise or forcing the application to perform functions not intended.

9.4% CWE-502

Deserialization of Untrusted Data

The application deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

8.5% CWE-285

Insufficient Authorization

Access control enforces policy such that users cannot act outside of their intended permissions. Applications were found with insufficient controls leading to unauthorized access of data or functionality.

7.6% CWE-200

Administrative Functionality Exposed

Administrator consoles provide access to privileged functionality which should not be internet-accessible, except by authorized hosts or networks. Such web pages occasionally suffer from known security weaknesses and must themselves be patched regularly. Password based attacks could also be used and if successful aid an attacker in compromising this host.

5.4% CWE-434

Malicious File Upload

Uploaded viruses and malware could later be downloaded by users of the application. Such malware can cause partial or complete compromise of a network that the host resides on.

3.6% CWE-200

Information Disclosure

The application exposed unnecessary sensitive information. Types of information considered sensitive include: Internal IP addresses, Physical paths on the host, Detailed platform information, Domain Information, etc.

3.1% CWE-77

Remote Command Injection

The application constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.

3.1% CWE-1329

Unsupported/Deprecated System

An application component is no longer supported. If the component is discovered to contain a vulnerability or critical bug, the issue cannot be fixed using an update or patch.

Web Applications

Medium Severity Vulnerabilities

Server-side Request Forgery (SSRF) was significant allowing attackers to interact with arbitrary external resources.

Cross-Site Scripting - XSS (reflected) at 19.1% is a common vulnerability whose prevalence does not seem to wane.

The most commonly found medium severity vulnerabilities across the application/web layer. "Medium Severity" vulnerabilities are defined by the Edgescan Validated Security Score (EVSS) which is a combination of analytics and expert validation.

19.1% CWE-79, CWE-725
Cross-Site Scripting - XSS (reflected)

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request which, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that users session with the application.

18.2% CWE-918
Server-Side Request Forgery

SSRF is an attack that abuses an application to interact with a privileged network or the server itself.

10.4% CWE-942
HTML5 Cross-Origin Resource Sharing

CORS, when misconfigured, can enable an attacker to bypass it and make the client browser act as a proxy between a malicious website and the target web application.

7.6% CWE-204
User Enumeration

When a failed log-in attempt is made, enumeration of the username can occur if the server returns a non-generic response.

6.8% CWE-643,CWE-91
Xpath Injection

Similar to SQL Injection, XPath Injection attacks occur when a website uses user-supplied information to construct an XPath query for XML data.

3.4% CWE-521
Weak Password Policy

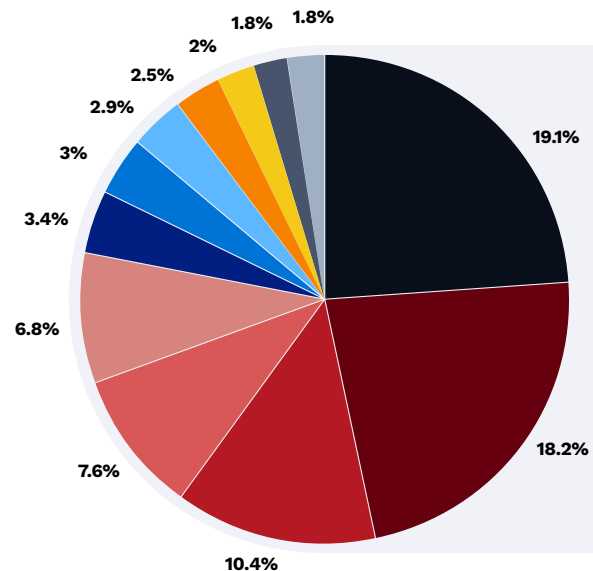
Poor password controls such as no MFA, Default Credentials etc.

3% CWE-419,CWE-284
Administrative Interface Exposed

Administrator consoles provide access to privileged functionality which should not be internet-accessible, except by authorized hosts or networks. Such web pages occasionally suffer from known security weaknesses and must themselves be patched regularly. Password based attacks could also be used and if successful aid an attacker in compromising this host.

2.9% CWE-601
Open Redirection

Unvalidated redirects and forwards are possible when a web application accepts untrusted input that could cause the web application to redirect to an arbitrary location.



2.5% CWE-200
Information Disclosure

The application exposed unnecessary sensitive information. Types of information considered sensitive include: internal IP addresses, physical paths on the host, detailed platform information, domain information, etc.

2% CWE-613
Insufficient Session Timeout

Insufficient session expiration by the web application increases the exposure to other session-based attacks.

1.8% CWE-644
Host Header Injection

Without proper validation of the host header, an application is vulnerable to a number of types of attack.

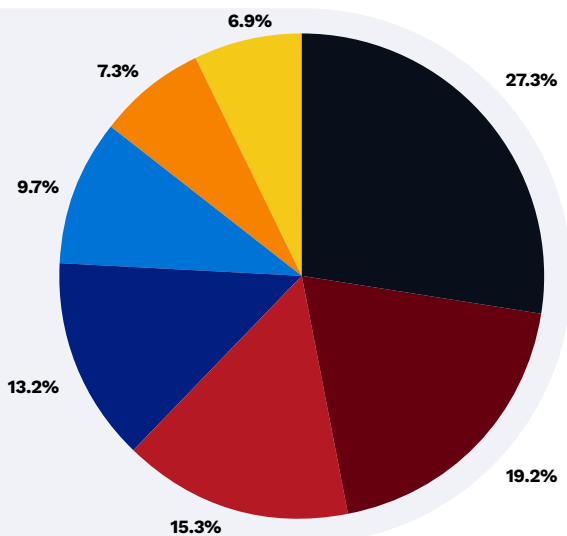
1.8% CWE-1104,CWE-1329
Vulnerable Wordpress Version

The version of the Wordpress deployed is known to be vulnerable.

API Critical and High Severity Vulnerabilities

An Application Programming Interface (API) is a way for two or more computer programs to communicate with each other. It is a type of software interface, offering a service to other pieces of software. API's have become very

popular but cyber security approaches to API's have been lacking. Using a custom security tool built for API assessments is of key importance, as there are many differences between API's and Web Applications.



Most Common High and Critical severity vulnerabilities discovered

Percentage of critical severity vulnerabilities discovered across all API's assessed in 2022. Edgescan validates vulnerabilities based on context of the unique issue and does not always tally with CVSS scoring.

CWE/OWASP: Common Weakness Enumeration/OWASP API Top 10 Reference.

27.3% ————— CWE-79, CWE-725/API8:2019

Injection Attacks

SQL, NoSQL, LDAP, OS Injections, Code Injections, ORM based vulnerabilities, Parsers such as XML, Traversal based attacks.

19.2% ————— CWE-770/API4:2019

Lack of Resources and Rate Limiting

The API does not restrict the number or frequency of requests from a particular API client. This can be abused to make thousands of API calls per second, or request hundred or thousands of data records at once, resulting in a Denial of Service condition. This weakness also enables arbitrary scraping of other parties API's and violate fair usage agreements.

15.3% ————— API2:2019/CWE-287

Broken Authentication

Weak authentication allowing compromise of authentication tokens or exploitation of common implementation flaws to assume other user's identity or bypass authentication completely, compromising systems ability to identify the client/user, compromises API security overall.

13.2% ————— CWE-639 / API1:2019

Broken Object Level Authorization (BOLA)

AKA insecure direct object reference (IDOR). As its name implies, the ability to directly access resources without privileges or authorization.

9.7% ————— CWE-22, CWE-23, CWE-200,CWE-269, CWE-250 / API3:2019

Excessive Data Exposure (Information Disclosure)

Exposure of all object properties of an API endpoint without consideration for use-case or requirement. Exposure of sensitive data.

7.3% ————— CWE-915 / API6:2019

Mass Assignment

API does not control which object attributes can be modified providing the potential for access to opaque data, outcomes or functions. This can be used to create new parameters that were never intended which in turn creates or overwrites new variable or objects in program code.

6.9% ————— CWE-285 / API5:2019

Broken Function Level Authorization

Admin or sensitive functions exposed in error to unauthorized clients resulting in data disclosure or privileged execution for unauthorized API clients. Could result in an overly large attack surface and unintended exposure risk.



“

**You control
your own
wins and
losses”**

Maria Sharapova

Vulnerability Severity

EPSS, CISA KEV, and 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?

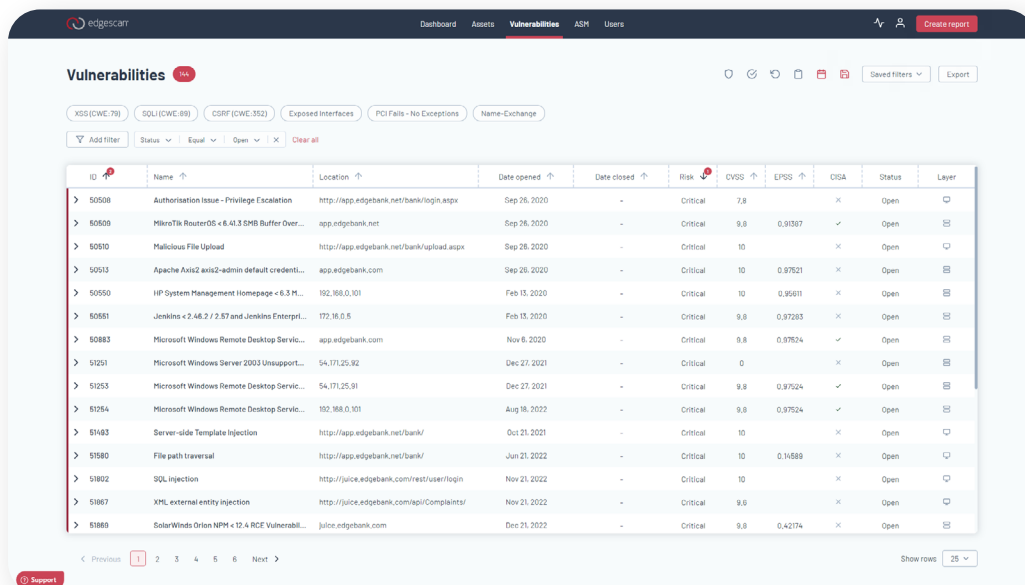
CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the [Known Exploited Vulnerability \(KEV\) catalog](#).

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 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.



ID	Name	Location	Date opened	Date closed	Risk	CVSS	EPSS	CISA	Status	Layer
50508	Authorisation Issue - Privilege Escalation	http://app.edgescan.net/bank/login.aspx	Sep 26, 2020	-	Critical	7.8		×	Open	
50506	Mikrotik RouterOS < 6.43.3 SMB Buffer Over...	app.edgescan.net	Sep 26, 2020	-	Critical	9.8	0.91597	✓	Open	
50510	Malicious File Upload	http://app.edgescan.net/bank/upload.aspx	Sep 26, 2020	-	Critical	10		×	Open	
50513	Apache Axis2 axis2-admin default creden...	app.edgescan.com	Sep 29, 2020	-	Critical	10	0.97521	×	Open	
50550	HP System Management Homepage < 6.3 M...	192.168.0.101	Feb 13, 2020	-	Critical	10	0.95611	×	Open	
50551	Jenkins < 2.46.2 / 2.87 and Jenkins Enterpr...	172.16.0.5	Feb 13, 2020	-	Critical	9.8	0.97283	×	Open	
50883	Microsoft Windows Remote Desktop Servic...	app.edgescan.com	Nov 6, 2020	-	Critical	9.8	0.97524	✓	Open	
51251	Microsoft Windows Server 2003 Unsupport...	54.171.25.92	Dec 27, 2021	-	Critical	0		×	Open	
51253	Microsoft Windows Remote Desktop Servic...	54.171.25.91	Dec 27, 2021	-	Critical	9.8	0.97524	✓	Open	
51254	Microsoft Windows Remote Desktop Servic...	192.168.0.101	Aug 18, 2022	-	Critical	9.8	0.97524	✓	Open	
51483	Server-side Template Injection	http://app.edgescan.net/bank/	Oct 21, 2021	-	Critical	10		×	Open	
51580	File path traversal	http://app.edgescan.net/bank/	Jun 21, 2022	-	Critical	10	0.16589	×	Open	
51802	SQL injection	http://juice.edgescan.com/rest/user/login	Nov 21, 2022	-	Critical	10		×	Open	
51867	XML external entity injection	http://juice.edgescan.com/api/Complaints/	Nov 21, 2022	-	Critical	9.6		×	Open	
51869	SolarWinds Orion NPM < 12.4 RCE Vulnerabil...	juice.edgescan.com	Dec 21, 2022	-	Critical	9.8	0.42174	×	Open	

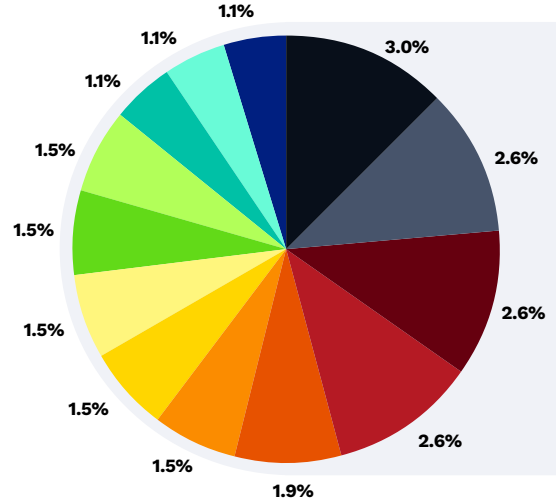
Internet Facing Vulnerabilities

Critical Severity

Critical Severity vulnerabilities discovered last year ordered by frequency.

Looking at vulnerabilities from a full stack perspective, we list the most common critical severity vulnerabilities found on internet-facing systems. The % column on the far left is the percentage of all critical severity vulnerabilities discovered. The CVSS score are undoubtedly high but not all vulnerabilities are listed on the CISA KEV or have a high probability via EPSS.

Note which are listed on the CISA KEV and the corresponding EPSS Score – In some cases the EPSS depicts a low probability of exploitation but it being on the CISA KEV means it is/has been exploited.



	Name	CVSS Score	CVE	CWE	On CISA KEV	CVE On CISA KEV	EPSS
3.0%	Apache Multiple Log4j Vulnerabilities (Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
2.6%	OS End Of Life Detection	10			FALSE		
2.6%	WordPress Elegant Themes Divi Theme 3.0 <= 4.5.2 Authenticated Arbitrary File Upload Vulnerability	9	CVE-2020-35945		FALSE		0.00885
2.6%	MariaDB End Of Life Detection (Windows)	10			FALSE		
1.9%	PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Windows	9.8	CVE-2021-21708	CWE-416	FALSE		0.00954
1.5%	Magento 2.3.3-p1 <= 2.3.7-p2, 2.4.x <= 2.4.3-p1 Multiple RCE Vulnerabilities (APSB22-12)	9.8	CVE-2022-24086, CVE-2022-24087	CWE-20	TRUE	CVE-2022-24086	0.35544
1.5%	PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update	9.8	CVE-2022-31630, CVE-2022-37454	CWE-125, CWE-190	FALSE		0.03806
1.5%	PHP Multiple Vulnerabilities (Feb 2019) - Windows	9.8	CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024	CWE-125, CWE-416	FALSE		0.02686
1.5%	Microsoft Exchange Server 2016 / 2019 Multiple Vulnerabilities (KB5007012) - Remote Known Vulnerable Versions Check	9.6	CVE-2021-26427, CVE-2021-34453, CVE-2021-41348, CVE-2021-41350	CWE-269	FALSE		0.02427
1.5%	Microsoft Exchange Server 2013 / 2016 / 2019 Multiple Vulnerabilities (KB5008631) - Unreliable Remote Version Check	9	CVE-2022-21846, CVE-2022-21855, CVE-2022-21969	CWE-94	FALSE		0.01877
1.1%	SAP Multiple Products Request Smuggling and Request Concatenation Vulnerability (ICMAD, 3123396) - Active Check	10	CVE-2022-22536	CWE-444	TRUE	CVE-2022-22536	0.19548
1.1%	PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)	9.8	CVE-2018-7584	CWE-119	FALSE		0.18327
1.1%	Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Windows	9.8	CVE-2021-44790	CWE-787	FALSE		0.07767

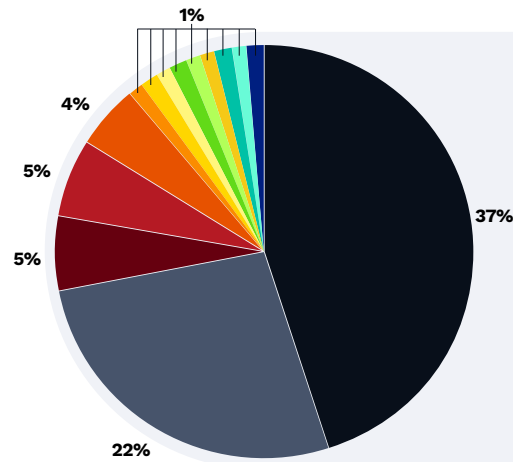
The mapping between CVSS, CISA KEV and EPSS is important to note. CISA KEV and EPSS do not appear to be aligned 100% of the time. High CVSS scores do not necessarily mean remediation is considered high priority. Some CISA KEV vulnerabilities have a low EPSS score. Conclusion: we need multiple viewpoints to determine priority.

Internet Facing Vulnerabilities

High Severity

High Severity vulnerabilities discovered last year ordered by frequency.

Looking at vulnerabilities from a full stack perspective we list the most common high severity vulnerabilities found on internet facing systems. The % column on the far left is the percentage of all high severity vulnerabilities discovered. This list contains a vast array of cryptographic vulnerabilities. In addition, exposed databases and vulnerable Microsoft Exchange servers make the list in this years report and are worth noting as they are actively exploited.



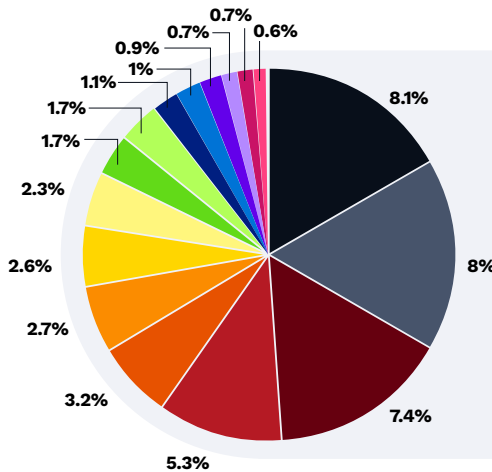
	Name	CVSS	CVE	CWE	On CISA KEV	CVE On CISA KEV	EPSS
37%	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	7.5	CVE-2016-2183	CWE-200	FALSE	CVE-2021-44228	0.34498
22%	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	7.5	CVE-2002-20001	CWE-400	FALSE		0.26127
5%	OpenSSH <= 8.6 Command Injection Vulnerability	7.8	CVE-2020-15778	CWE-78	FALSE		0.01787
5%	OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability	7	CVE-2021-41617	CWE-269	FALSE		0.01282
4%	OpenSSH < 8.1 Integer Overflow Vulnerability	7.8	CVE-2019-16905	CWE-190	FALSE		0.01864
1%	Database Open Access Vulnerability	7.5		CWE-497	FALSE	CVE-2022-24086	
1%	Sensitive File Disclosure (HTTP)	7.5		CWE-200	FALSE		
1%	OpenSSL 'ChangeCipherSpec' MITM Vulnerability	7.4	CVE-2014-0224	CWE-326	FALSE		0.95231
1%	nginx 0.6.18 - 1.20.0 1-byte Memory Overwrite Vulnerability	7.7	CVE-2021-23017	CWE-193	FALSE		0.48051
1%	nginx <= 1.21.1 Information Disclosure Vulnerability	7.5	CVE-2013-0337	CWE-264	FALSE		0.01018
1%	WordPress Advanced Custom Fields Pro Plugin 5.x < 5.12.3 File Upload Vulnerability	8.8	CVE-2022-2594	CWE-434	FALSE		0.00885
1%	Microsoft Exchange Server OWA Multiple Vulnerabilities (Sep 2022, ProxyNotShell)	8.8	CVE-2022-41040, CVE-2022-41082	CWE-269	TRUE	CVE-2022-41040, CVE-2022-41082	0.31667
1%	Open Ports	7.5	CVE-2011-3190, CVE-2011-3375, CVE-2012-0022	CWE-189, CWE-200, CWE-264	FALSE		0.07344
1%	Wowza Streaming Engine <= 4.8.11+5 Multiple Vulnerabilities	8.1	CVE-2021-35491, CVE-2021-35492	CWE-352, CWE-770	FALSE		0.06511

Microsoft Vulnerabilities CVE-2022-41040, CVE-2022-41082 were uncommon at 1% but are listed on the CISA KEV. OpenSSL 'Change-CipherSpec' MITM Vulnerability CVE-2014-0224 has an EPSS score of 95% but again an uncommon vulnerability at 1% and not listed on the CISA KEV.

Non-Internet Facing Vulnerabilities

Critical Severity

Critical severity vulnerabilities not exposed to the public Internet. Once a perimeter is breached an attacker is typically faced with a wide array of insecure systems. Internal/Non-Internet facing networks are generally weaker and easier to exploit. This provides ransomware threat actors with ample opportunity to pivot across an internal network due to general poor security.



Mozilla Firefox Security Updates (mfsa2022-24) - Windows
8.1% CVSS **9.8**

CVE-2022-2200, CVE-2022-34468, CVE-2022-34470, CVE-2022-34471, CVE-2022-34472, CVE-2022-34473, CVE-2022-34474, CVE-2022-34475, CVE-2022-34476, CVE-2022-34477, CVE-2022-34478, CVE-2022-34480, CVE-2022-34481, CVE-2022-34482, CVE-2022-34483, CVE-2022-34484, CVE-2022-34485, CVE-2022-0511, CVE-2022-22753, CVE-2022-22754, CVE-2022-22755, CVE-2022-22756, CVE-2022-22757, CVE-2022-22759, CVE-2022-22760, CVE-2022-22761, CVE-2022-22764	On CISA KEV	False
CWE-1321, CWE-190, CWE-416, CWE-601, CWE-617, CWE-787, CWE-79, CWE-824	EPSS	0.23331

Adobe Acrobat Various Vulnerabilities
8% CVSS **10**

CVE-2009-0193, CVE-2009-0658, CVE-2009-0927, CVE-2009-0928, CVE-2009-1061, CVE-2009-1062, CVE-2019-7140, CVE-2019-7141, CVE-2019-7142, CVE-2019-7143, CVE-2019-7144, CVE-2019-7145, CVE-2019-7758, CVE-2019-7759, CVE-2019-7760, CVE-2019-7761, CVE-2019-7762, CVE-2019-7763, CVE-2019-7764, CVE-2019-7765, CVE-2019-7766, CVE-2019-7767, CVE-2019-7768, CVE-2019-7769, CVE-2019-7770, CVE-2019-7771, CVE-2019-7772, CVE-2019-7773, CVE-2019-7774, CVE-2019-7775, CVE-2019-7776, CVE-2019-7777, CVE-2019-7778, CVE-2019-7779, CVE-2019-7780, CVE-2019-7781, CVE-2019-7782, CVE-2019-7783, CVE-2019-7784, CVE-2019-7785, CVE-2019-7786, CVE-2019-7787, CVE-2019-7788, CVE-2012-1535, CVE-2019-7789, CVE-2019-7790, CVE-2019-7791, CVE-2019-7792, CVE-2019-7793, CVE-2019-7794, CVE-2019-7795, CVE-2019-7796, CVE-2019-7797, CVE-2019-7798, CVE-2019-7799, CVE-2019-7800, CVE-2019-7801, CVE-2019-7802, CVE-2019-7803, CVE-2019-7804, CVE-2019-7805, CVE-2019-7806, CVE-2019-7807, CVE-2019-7808, CVE-2019-7809, CVE-2019-7810, CVE-2019-7811, CVE-2019-7812, CVE-2019-7813, CVE-2019-7814, CVE-2019-7817, CVE-2019-7818, CVE-2019-7820, CVE-2019-7821, CVE-2019-7822, CVE-2019-7823, CVE-2019-7824, CVE-2019-7825, CVE-2019-7826, CVE-2019-7827, CVE-2019-7828, CVE-2019-7829, CVE-2019-7830, CVE-2019-7831, CVE-2019-7832, CVE-2019-7833, CVE-2019-7834, CVE-2019-7835, CVE-2019-7836, CVE-2019-7841	On CISA KEV	True
CWE-119, CWE-20	EPSS	0.86734

Mozilla Firefox Security Update Various
7.4% CVSS **9.6**

CVE-2022-0511, CVE-2022-22753, CVE-2022-22754, CVE-2022-22755, CVE-2022-22756, CVE-2022-22757, CVE-2022-22759, CVE-2022-22760, CVE-2022-22761, CVE-2022-22764	On CISA KEV	False
CWE-119, CWE-20, CWE-209, CWE-367, CWE-672, CWE-787, CWE-863	EPSS	0.01018

Oracle Java SE Security Updates (apr2019-5072813) - Windows
5.3% CVSS **9**

CVE-2019-2699	EPSS	0.00954	On CISA KEV	False
---------------	------	----------------	-------------	-------

Adobe Flash Player Various Vulnerabilities
3.2% CVSS **10**

CVE-2014-0497, CVE-2018-4877, CVE-2018-4878, CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0971, CVE-2016-0972, CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, CVE-2016-0981, CVE-2016-0982, CVE-2016-0983, CVE-2016-0984, CVE-2016-0985, CVE-2018-15982, CVE-2018-15983	On CISA KEV	True
CWE-189	EPSS	0.9405

Microsoft SQL Server Unsupported Version Detection
2.7% CVSS **10** On CISA KEV **False**

OS End Of Life Detection
2.6% CVSS **10** On CISA KEV **False**

SUSE: Various Security Advisories
2.3% CVSS **9.8**

CVE-2019-18902, CVE-2019-18903, CVE-2020-7216, CVE-2020-7217	EPSS	0.01156	On CISA KEV	False
CWE-401, CWE-416, CWE-772				

Intel Active Management Technology Multiple Vulnerabilities (INTEL-SA-00295)
1.7% CVSS **9,8**

CVE-2020-0531, CVE-2020-0532, CVE-2020-0537, CVE-2020-0538, CVE-2020-0540, CVE-2020-0594, CVE-2020-0595, CVE-2020-0596, CVE-2020-11899, CVE-2020-11900, CVE-2020-12356, CVE-2020-8746, CVE-2020-8747, CVE-2020-8749, CVE-2020-8752, CVE-2020-8753, CVE-2020-8754, CVE-2020-8755, CVE-2020-8760	On CISA KEV	True
CWE-125, CWE-20, CWE-415, CWE-416, CWE-522	EPSS	0.00885

MortBay / Eclipse Jetty End of Life (EOL) Detection - Windows
1.7% CVSS **10** On CISA KEV **False**

Eclipse Jetty Server Fake Pipeline Request Security Bypass Vulnerability (Windows)
1.1% CVSS **9,8**

CVE-2017-7658	On CISA KEV	False
CWE-444	EPSS	0.02686

Check_MK End of Life (EOL) Detection
1% CVSS **10** On CISA KEV **False**

Cisco Smart Install Protocol Misuse
0.9% CVSS **10** On CISA KEV **False**

Apache Tomcat AJP RCE Vulnerability (Ghostcat)
0.7% CVSS **9,8**

CVE-2020-1938	CWE-269	
EPSS	0.96554	CVE-2020-1938 On CISA KEV True

SUSE: Security Advisory (SUSE-SU-2022:3466-1)
0.7% CVSS **9,8**

CVE-2022-40674	On CISA KEV	False
CWE-416	EPSS	0.17166

HTTP Brute Force Logins With Default Credentials
0.6% CVSS **9** On CISA KEV **False**

Non-Internet Facing Vulnerabilities

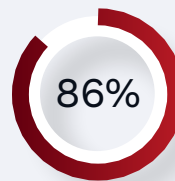
Critical Severity

Highlights



Mozilla Firefox and Adobe top the list with multiple CVE's. The Adobe vulnerabilities are listed on the CISA KEV and have an EPSS score of 86%.

EPSS Score

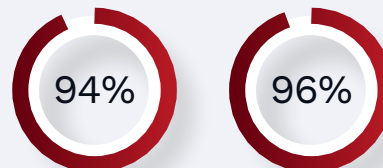


Adobe



Adobe Flash, Apache and Intel vulnerabilities also have CISA KEV entries. The Adobe Flash vulnerability also has an EPSS score of 94% and Apache EPSS score of 96% albeit not as common a weakness.

EPSS Score



Flash

Apache

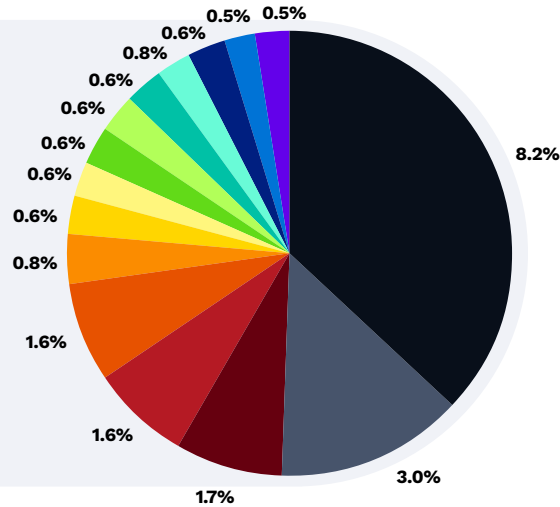


The idea that “it’s behind the firewall so not a priority” is a mistake. As we can see, three of the most common vulnerabilities are on the CISA KEV list with high EPSS scores meaning a high probability of exploitation.

Once an organisations perimeter is breached its vulnerabilities such as those listed, are exploited to pivot and spread across the internal network.

Non-Internet Facing Vulnerabilities

High Severity



Mozilla Firefox Security Updates (mfsa2022-24) - Windows
8.2% CVSS **7.5**

CVE-2016-2183	On CISA KEV	False
CWE-200	EPSS	0.34498

Windows IExpress Untrusted Search Path Vulnerability
3.0% CVSS **7.8**

CVE-2018-0598	On CISA KEV	False
CWE-426	EPSS	0.10418

SNMP Agent Default Community Names
1.7% CVSS **7.5**

CVE-1999-0517	On CISA KEV	False
CWE-264	EPSS	0.00885

Microsoft OneDrive Privilege Escalation Vulnerability - July 2020
1.6% CVSS **7.8**

CVE-2020-1465	On CISA KEV	False
CWE-269	EPSS	0.0115

Microsoft OneDrive Multiple Vulnerabilities - Sep 2020
1.6% CVSS **7.1**

CVE-2020-16851, CVE-2020-16852, CVE-2020-16853	On CISA KEV	False
CWE-269, CWE-59	EPSS	0.0115

Adobe Reader DC Continuous Security Update (APSB22-16) - Windows
0.8% CVSS **7.8**

CVE-2022-24101, CVE-2022-24102, CVE-2022-24103, CVE-2022-24104, CVE-2022-27785, CVE-2022-27786, CVE-2022-27787, CVE-2022-27788, CVE-2022-27789, CVE-2022-27790, CVE-2022-27791, CVE-2022-27792, CVE-2022-27793, CVE-2022-27794, CVE-2022-27795, CVE-2022-27796, CVE-2022-27797, CVE-2022-27798, CVE-2022-27799, CVE-2022-27800, CVE-2022-27801, CVE-2022-27802, CVE-2022-28230, CVE-2022-28231, CVE-2022-28232, CVE-2022-28233, CVE-2022-28234, CVE-2022-28235, CVE-2022-28236, CVE-2022-28237, CVE-2022-28238, CVE-2022-28239, CVE-2022-28240, CVE-2022-28241, CVE-2022-28242, CVE-2022-28243, CVE-2022-28244, CVE-2022-28245, CVE-2022-28246, CVE-2022-28247, CVE-2022-28248, CVE-2022-28249, CVE-2022-28250, CVE-2022-28251, CVE-2022-28252, CVE-2022-28253, CVE-2022-28254, CVE-2022-28255, CVE-2022-28256, CVE-2022-28257, CVE-2022-28258, CVE-2022-28259, CVE-2022-28260, CVE-2022-28261, CVE-2022-28262, CVE-2022-28263, CVE-2022-28264, CVE-2022-28265, CVE-2022-28266, CVE-2022-28267, CVE-2022-28268, CVE-2022-28269, CVE-2022-28837, CVE-2022-28838	On CISA KEV	False
CWE-125, CWE-416, CWE-427, CWE-787, CWE-824	EPSS	0.01223

Microsoft Windows Defender Antimalware Platform Remote Code Execution Vulnerability - Jan 2021

0.6%	CVSS 7.8
CVE-2021-1647	On CISA KEV True
CWE-131	EPSS 0.01877

Microsoft Defender Antimalware Platform Multiple Elevation of Privilege Vulnerabilities - June 2020

0.6%	CVSS 7.8
CVE-2020-1163, CVE-2020-1170	On CISA KEV False
CWE-269	EPSS 0.01178

Microsoft Defender Antimalware Platform Elevation of Privilege Vulnerability - April 2020

0.6%	CVSS 7.8
CVE-2020-0835	On CISA KEV False
CWE-269	EPSS 0.0115

Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)

0.6%	CVSS 7.8
CVE-2022-30190	On CISA KEV False
CWE-269	EPSS 0.69589

Microsoft Office 365 (2016 Click-to-Run) Multiple Vulnerabilities - Nov22

0.6%	CVSS 7.8
CVE-2022-41060, CVE-2022-41061, CVE-2022-41063, CVE-2022-41103, CVE-2022-41104, CVE-2022-41105, CVE-2022-41106, CVE-2022-41107	On CISA KEV False
CWE-269	EPSS 0.04475

Adobe Reader DC Continuous Security Update (APSB22-32) - Windows

0.8%	CVSS 7.8
CVE-2022-34215, CVE-2022-34216, CVE-2022-34217, CVE-2022-34219, CVE-2022-34220, CVE-2022-34221, CVE-2022-34222, CVE-2022-34223, CVE-2022-34224, CVE-2022-34225, CVE-2022-34226, CVE-2022-34227, CVE-2022-34228, CVE-2022-34229, CVE-2022-34230, CVE-2022-34232, CVE-2022-34233, CVE-2022-34234, CVE-2022-34236, CVE-2022-34237, CVE-2022-34238, CVE-2022-34239, CVE-2022-35669	On CISA KEV False
CWE-125, CWE-416, CWE-787, CWE-824, CWE-843	EPSS 0.01223

Adobe Reader DC Continuous Security Update (APSB22-39) - Windows

0.6%	CVSS 7.8
CVE-2022-35665, CVE-2022-35666, CVE-2022-35667, CVE-2022-35668, CVE-2022-35670, CVE-2022-35671, CVE-2022-35678	On CISA KEV False
CWE-125, CWE-20, CWE-416, CWE-787	EPSS 0.01223

Oracle Java SE Security Update (oct2021) 01 - Windows

0.5%	CVSS 8.6
CVE-2021-3517, CVE-2021-3522, CVE-2021-35560	On CISA KEV False
CWE-125, CWE-787	EPSS 0.02686

Oracle Java SE Security Update (jul2021) 02 - Windows

0.5%	CVSS 7.5
CVE-2021-2388	On CISA KEV False
CWE-125, CWE-20, CWE-416, CWE-787	EPSS 0.01108

The continuing challenge of Ransomware attacks can be reduced and pivot/breach can be made more difficult if additional effort was focused on non-Internet facing systems, the "soft-underbelly" of our enterprise IT security. Internal system security is all about resilience. Lets make it hard for the enemy!

Most Common Vulnerabilities listed on the CISA KEV

The below depicts the most commonly found vulnerabilities which are listed in the “Known Exploited Vulnerabilities” Catalogue (KEV). Vulnerabilities in Windows Defender and Windows Support applications were the most

commonly found. Such weaknesses provide the ability to breach and take-over windows systems. This list covers both Internet and non Internet facing systems.

9.4% Severity **High** | EPSS **0.01877**

Microsoft Windows Defender Antimalware Platform Remote Code Execution Vulnerability - Jan 2021

CVE-2021-1647

9.2% Severity **High** | EPSS **0.69589**

Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)

CVE-2022-30190

8.4% Severity **Critical** | EPSS **0.96554**

SUSE: Security Advisory (SUSE-SU-2019:2949-1)(SUSE-SU-2020:1272-1)(SUSE-SU-2020:2721-1) (SUSE-SU-2020:2998-1)(SUSE-SU-2021:0226-1) (SUSE-SU-2021:1273-1) (SUSE-SU-2022:0189-1) (SUSE-SU-2022:0762-1)

CVE-2021-0920, CVE-2021-3156, CVE-2021-3156, CVE-2020-15999, CVE-2021-4034, CVE-2021-0920, CVE-2022-0847, CVE-2020-1938, CVE-2021-40438

7.6% Severity **Critical** | EPSS **0.01055**

Google Chrome Security Update (stable-channel-update-for-desktop_11-2020-11) - Windows

CVE-2020-16013, CVE-2020-16017

7.1% Severity **Critical** | EPSS **0.00885**

Mozilla Firefox Multiple Vulnerabilities - Windows

CVE-2022-26485, CVE-2022-26486CVE-2020-6819, CVE-2020-6820CVE-2019-11708

4.4% Severity **High** | EPSS **0.58695**

Sudo Heap-Based Buffer Overflow Vulnerability (Baron Samedit) - Active Check

CVE-2021-3156

3.6% Severity **Critical** | EPSS **0.75301**

Oracle Java SE Java Runtime Environment Code Execution Vulnerability - (Windows)

CVE-2015-4902CVE-2015-2590CVE-2020-14882, CVE-2020-14750CVE-2012-1723CVE-2013-0431CVE-2010-0840CVE-2012-0507CVE-2011-3544CVE-2013-2465CVE-2018-2628CVE-2019-2725CVE-2021-35587

2.3% Severity **Critical** | EPSS **0.75301**

Microsoft IE And Microsoft Edge Multiple RCE Vulnerabilities

CVE-2018-4878CVE-2018-5002CVE-2016-0984CVE-2016-1010CVE-2016-1019CVE-2016-4117CVE-2016-4171CVE-2015-5122, CVE-2015-5123CVE-2015-8651CVE-2016-7855CVE-2016-7892

1.9% Severity **High** | EPSS **0.75301**

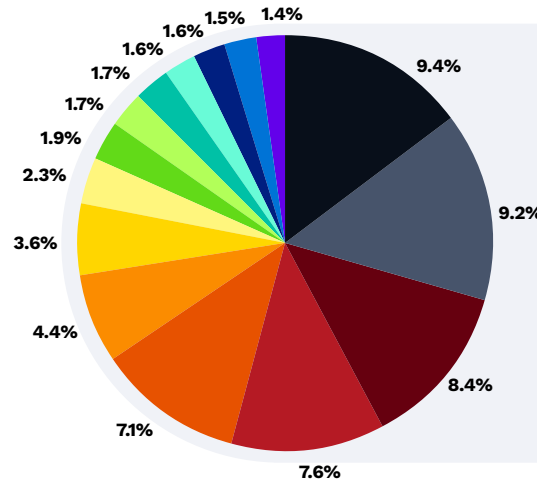
Adobe Flash Player Multiple Vulnerabilities - (Windows)

CVE-2012-1535CVE-2015-3113CVE-2018-4878CVE-2015-3043CVE-2012-0754, CVE-2012-0767CVE-2012-5054CVE-2015-8651CVE-2016-0984CVE-2015-5122, CVE-2015-5123CVE-2012-2034CVE-2014-8439CVE-2014-9163CVE-2016-4117CVE-2016-1010CVE-2016-1019CVE-2016-4171CVE-2018-5002CVE-2018-15982CVE-2015-0313CVE-2015-5119CVE-2017-11292CVE-2010-1297

1.7% Severity **High** | EPSS **0.86056**

Microsoft Malware Protection Engine on Windows Defender Multiple Vulnerabilities

CVE-2017-8540



1.7% Severity **High** | EPSS **0.09099**

Microsoft Windows Multiple Vulnerabilities (KB4493474)(KB4499181) (KB4503279) (KB4507450) (KB4516068)(KB4520010) (KB4561608)(KB5000807)(KB5003173) (KB5003637)(KB5004237)(KB5004245)(KB5005033)(KB5005565)(KB5006670)

CVE-2021-40449, CVE-2021-40450, CVE-2021-41357CVE-2021-36955, CVE-2021-40444CVE-2021-34484, CVE-2021-34486, CVE-2021-36942, CVE-2021-36948CVE-2021-1675, CVE-2021-31199, CVE-2021-31201, CVE-2021-31955, CVE-2021-31956, CVE-2021-33739, CVE-2021-33742CVE-2021-31979, CVE-2021-33771, CVE-2021-34448CVE-2021-31166CVE-2022-24521, CVE-2022-26904CVE-2019-0880, CVE-2019-1129, CVE-2019-1130CVE-2019-1214, CVE-2019-1215, CVE-2019-1253CVE-2019-1315, CVE-2019-1367CVE-2020-0986CVE-2019-0863, CVE-2019-0903CVE-2021-1732CVE-2021-26411, CVE-2021-27085CVE-2019-0752, CVE-2019-0859, CVE-2019-0841, CVE-2019-0803CVE-2019-1064, CVE-2019-1069CVE-2022-41073, CVE-2022-41125, CVE-2022-41128CVE-2021-26411

1.6% Severity **Critical** | EPSS **0.96554**

Apache Tomcat AJP RCE Vulnerability (Ghostcat)

CVE-2020-1938

1.6% Severity **Critical** | EPSS **0.01537**

Intel Active Management Technology Multiple Vulnerabilities (INTEL-SA-00295)

CVE-2020-11899

1.5% Severity **Critical** | EPSS **0.19548**

SAP Multiple Products Request Smuggling and Request Concatenation Vulnerability (ICMAD, 3123396)

CVE-2022-22536

1.4% Severity **High** | EPSS **0.11196**

TeamViewer Multiple Vulnerabilities (CVE-2019-18988) - Windows

CVE-2019-18988

The % of all vulnerabilities on the CISA KEV: The percentage of all vulnerabilities discovered by Edgescan last year which happen to be listed on the CISA Exploitability Catalogue.

Note, not all vulnerabilities listed in the CISA KEV have a corresponding high EPSS score (High probability of breach). We need multiple sources of meta data to help prioritize remediation.

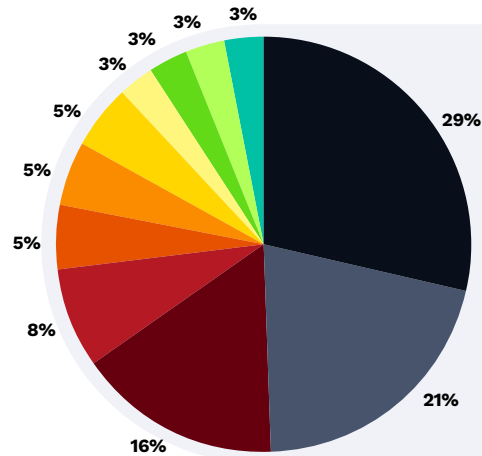
Highest Probability of Exploitation (EPSS)

Internet Facing

The highest probability (of attack) vulnerabilities discovered on public Internet facing systems last year based on the EPSS probability score which provides a value between 0.0 – 1.0 . (0=0%, 1=100% probability of attack).

The most common of the top EPSS vulnerabilities discovered was CVE-2014- 0224, OpenSSL ‘ChangeCipherSpec’ MiTM Vulnerability at 29% with an EPSS score of 95%.

Log4J vulnerabilities (Log4Shell), CVE-2021-44228, was the highest EPSS score at 97%, discovered in last year’s report.



	Name	CVSS	CVE	CWE	On CISA KEV	CVE On CISA KEV	EPSS
29%	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	7.4	CVE-2014-0224	CWE-326	FALSE		0.95231
21%	Wowza Streaming Engine < 4.8.17 Multiple Log4j Vulnerabilities (Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	
16%	MobileIron Core Multiple Log4j Vulnerabilities (Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
8%	Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows	9.8	CVE-2021-34798, CVE-2021-39275, CVE-2021-40438	CWE-476, CWE-787, CWE-918	TRUE	CVE-2021-40438	0.97224
5%	Elastic Elasticsearch Multiple Log4j Vulnerabilities (ESA-2021-31, Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
5%	SAP NetWeaver AS Java Multiple Vulnerabilities (2934135)	10	CVE-2020-6286, CVE-2020-6287	CWE-22, CWE-306	TRUE	CVE-2020-6287	0.95175
5%	Generic HTTP Directory Traversal	9.8	CVE-2010-2307, CVE-2010-4231, CVE-2014-2323, CVE-2015-5688, CVE-2017-16806, CVE-2018-14064, CVE-2018-18778, CVE-2018-7490, CVE-2019-20085, CVE-2020-24571, CVE-2020-5410, CVE-2021-3019, CVE-2021-40978, CVE-2021-41773, CVE-2021-42013	CWE-200, CWE-22, CWE-89	TRUE	CVE-2019-20085, CVE-2020-5410, CVE-2021-41773, CVE-2021-42013	0.93300
3%	PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability	9.8	CVE-2019-11043	CWE-787	TRUE	CVE-2019-11043	0.96000
3%	ManageEngine ADSelfService Plus < 6114 Authentication Bypass Vulnerability	9.8	CVE-2021-40539	CWE-287	TRUE	CVE-2021-40539	0.95954
3%	Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	10	CVE-2015-0240	CWE-17	FALSE		0.95138
3%	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution	10	CVE-2015-1635	CWE-94	TRUE	CVE-2015-1635	0.93779

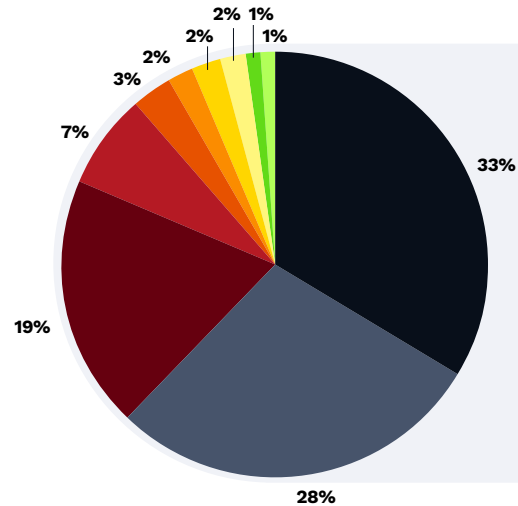
The above is an list of the most common high probability vulnerabilities discovered on Internet facing systems in the 12 months to December 2022.

The most common vulnerability (OpenSSL MiTM) at 29% has an EPSS score of 0.95 and a CVSS score of 7.4 but is not listed in the CISA catalogue.

Highest Probability of Exploitation (EPSS)

Non-Internet Facing

With an EPSS of 97% and a frequency of 33% of all “high probability of attack” vulnerabilities (for non-Internet facing systems), VMware CVE-2021-4428 should be considered a high priority vulnerability to address ASAP.



	Name	CVSS	CVE	CWE	On CISA KEV	CVE On CISA KEV	EPSS
33%	VMware vCenter Server 6.5, 6.7, 7.0 Multiple Log4j Vulnerabilities (VMSA-2021-0028, Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
28%	Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows	9.8	CVE-2021-34798, CVE-2021-39275, CVE-2021-40438	CWE-476, CWE-787, CWE-918	TRUE	CVE-2021-40438	
19%	Elastic Elasticsearch Multiple Log4j Vulnerabilities (ESA-2021-31, Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
7%	ManageEngine ADAudit Plus Multiple Log4j Vulnerabilities (Log4Shell)	10	CVE-2021-44228, CVE-2021-45046, CVE-2021-45105	CWE-20, CWE-400, CWE-502, CWE-674	TRUE	CVE-2021-44228	0.97095
3%	Ubiquiti UniFi Network < 6.5.54 Log4j RCE Vulnerability (Log4Shell)	10	CVE-2021-44228	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
2%	Apache Solr 7.x, 8.x Log4j RCE Vulnerability (Log4Shell)	10	CVE-2021-44228	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
2%	FedEx Ship Manager 340x - 3508 Multiple Log4j Vulnerabilities (Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
2%	Cisco Application Policy Infrastructure Controller Multiple Log4j Vulnerabilities (cisco-sa-apache-log4j-qRuKNEbd, Log4Shell)	10	CVE-2021-44228, CVE-2021-45046	CWE-20, CWE-400, CWE-502	TRUE	CVE-2021-44228	0.97095
1%	SUSE: Security Advisory (SUSE-SU-2021:3299-1)	9.8	CVE-2021-34798, CVE-2021-39275, CVE-2021-40438	CWE-476, CWE-787, CWE-918	TRUE	CVE-2021-40438	0.97224
1%	Atlassian Confluence RCE Vulnerability (CONFSERVER-67940)	9.8	CVE-2021-26084	CWE-74	TRUE	CVE-2021-26084	0.97974

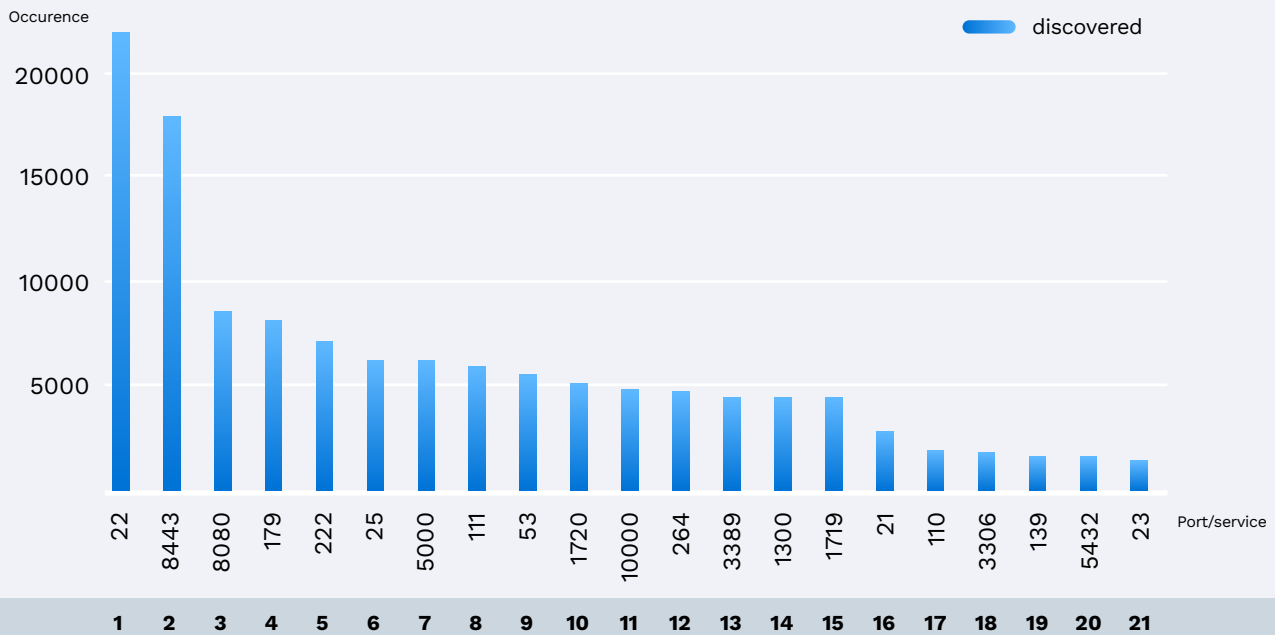
The above depicts the vulnerabilities with the highest EPSS (probability) and the associated % of occurrence which were discovered in 2022.

Both EPSS and CISA KEV are aligned (both high probability and listed in catalogue) as per the matrix above.

Attack Surface Management (ASM)

Exposure Landscape

Based on a sample of continuous scans the below describes the systems discovered to be exposed on the public Internet. (Standard web ports such as http 80 and https 443 are excluded).



Protocol	Notes
1	SSH Exposed remote Access Service. There were 90 CVE's reported relating to SSH in 2022
2	HTTP Potential Pre-production Web Service
3	HTTP Potential Pre-production Web Application
4	BGP Exposed Border Gateway Web Service. There were 17 CVE's reported relating to BGP in 2022
5	UDP UDP Service
6	SMTP Exposed SMTP Email Port.
7	UPnP Exposed Universal Plug and Play Service. There were 5 CVE's reported relating to UPnP in 2022
8	SUNRPC Exposed RPC service. There were 4 CVE's reported relating to SUNRPC in 2022
9	DNS DNS Service
10	H323 Exposed VOIP service. There were 8 CVE's reported relating to H323/SIP in 2022
11	NDMP Exposed Network Data Management Protocol
12	SecuRemote Checkpoint SecuRemote Service.
13	RDP Exposed Remote Login. There were 16 CVE's reported relating to RDP in 2022
14	H323 VOIP service. There were 8 CVE's reported relating to H323/SIP in 2022
15	SMB Exposed SMB Report. There were 18 CVE's reported relating to RDP in 2022
16	FTP File Transfer Service. There were 18 CVE's reported relating to FTP in 2022
17	POP3 Plain text Email Port Service
18	MYSQL Exposed Database
18	SMB Server Message Block
20	PostgreSQL Exposed Database
21	Telnet Exposed Remote Access

We still see exposed Databases and remote access services which are easily exploited for data theft, network breach or ransomware attacks.

Many of the exposed services of note have CVE's attributed to them in 2022.

SSH exposures were relatively common (21,910 exposures discovered). SSH had circa 90 new CVE's attributed to the protocol in 2022.

Remote Access exposures are a common attack vector for ransomware attacks as a first step in the attack chain.

“

**Victorious warriors
win first and then
go to war, while
defeated warriors go
to war first and then
seek to win”**

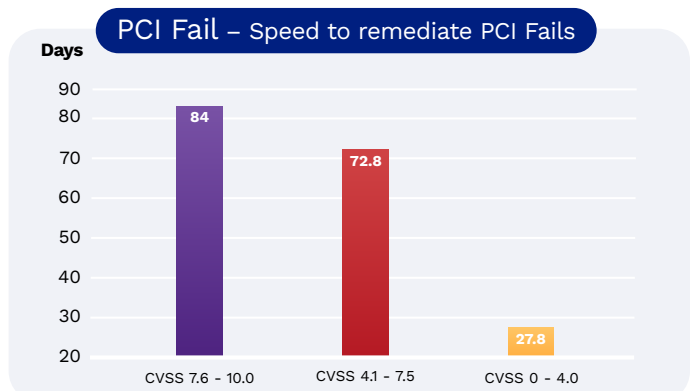
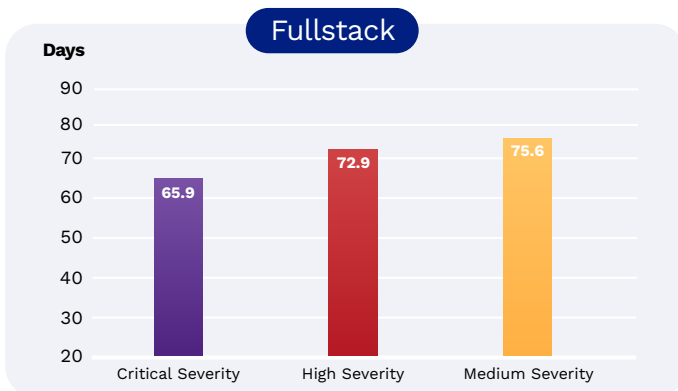
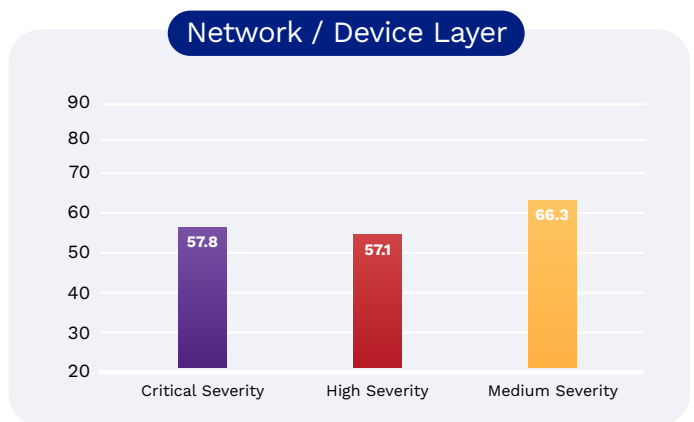
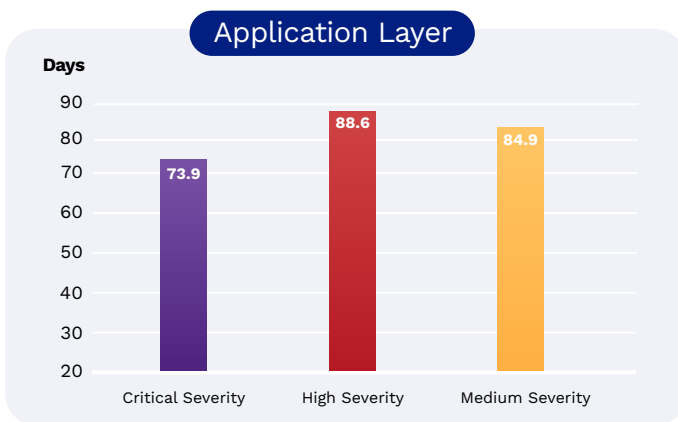
Sun Tzu






Mean Time to Remediate (MTTR)

Time it takes to fix Vulnerabilities across the Full Stack

The mean time in calendar days it takes to mitigate discovered vulnerabilities based on layer and severity. It is still taking in excess of 2 months in general to address known vulnerabilities.

Measuring and attempting to adhere to an internal remediation SLA (Service Level Agreement) may help measure and highlight serious vulnerabilities which remain open after a defined period of time.



-  The measurements include remediation and verification that the fixes are robust (including reassessments & retesting).
-  Mean time to Remediate (i.e. a code fix) for a critical risk on the web application/API layer is 73.9 days.
-  Mean time to Remediate (i.e. patch or reconfigure) a device/host layer critical risk is 57.8 days.
-  The quickest remediation on a vulnerability that was found was 0.25 days.
-  Edgescan has a Vulnerability Lifecycle SLA feature which measures vulnerability age and alerts you to vulnerabilities needing urgent attention. (<https://www.edgescan.com/new-edgescan-feature-sla/>).

MTTR by Industry

Mean Time to Remediate Vulnerabilities



Public Administration (NAICS* 92)

89 Days



Manufacturing (NAICS 31-33)

81 Days



Education Services (NAICS 61)

81 Days



Arts, Entertainment and Recreation (NAICS 71)

72 Days



Professional, Scientific & Technical Services (NAICS 54)

69 Days



Accommodation & Food Services (NAICS 72)

68 Days



Healthcare (NAICS 62)

63 Days



Information (NAICS 51)

57 Days



Retail (NAICS 44-45)

55 Days



Financial & Insurance (NAICS 52)

47 Days

For 2022 we examined ten different industries to report on their average rates of MTTR within that industry. We can see that the shortest MTTR can be seen in Financial & Insurance (NAICS 52): 47 days while the longest is Public Administration (NAICS 92): 89 days.

*Federal agencies use the North American Industry Classification System (NAICS) to classify businesses when collecting, analyzing, and publishing statistical data about the United States economy. This numeric coding system is also used for administrative, regulatory, contracting, and taxation purposes.

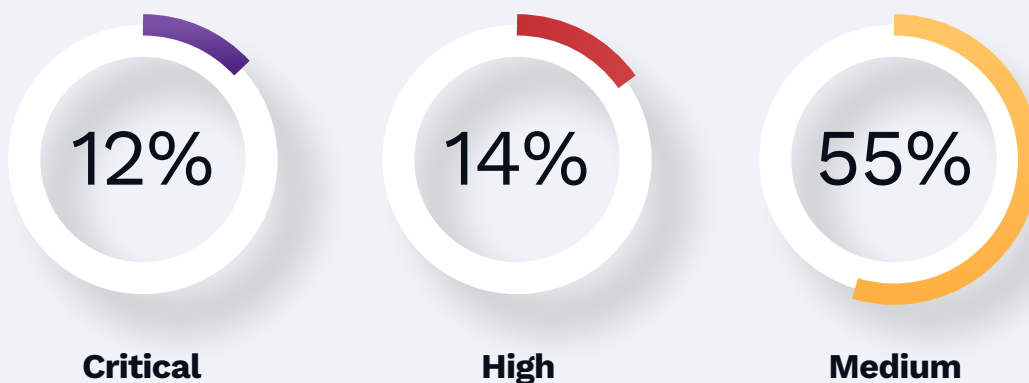
Risk Accepted

Most organizations maintain the concept of accepting known risks. There are lots of reasons why this is done and some common ones include; the presence of some other compensating control, acknowledgement that the risk is impractically low, or that an upcoming change will remove the risk completely. Edgescan clients with appropriate privileges can “Risk-Accept” vulnerabilities in the platform.

A Risk-Accepted issue puts a discovered vulnerability in a “non-closed” state so that it is tracked but not used to calculate risks scores in the organization. The below table shows a list of the most common vulnerability types that our clients tend to “Risk-Accept”.

Risk Accepted Overall

Most Common by severity



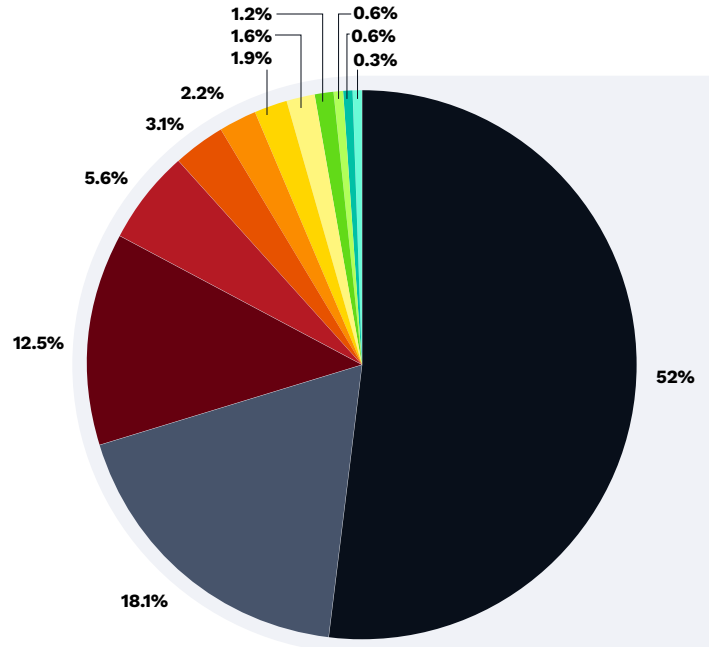
12% of all Risk accepted vulnerabilities in **2022** were considered (in isolation) **Critical risk!!!** – This is surprising.

When considered in isolation and not considering any compensating controls, many of the High and Critical Severity vulnerabilities which were risk accepted in 2022 are commonly used by ransomware and criminal threat agents to pivot across internal and external facing networks.

Critical Severity:

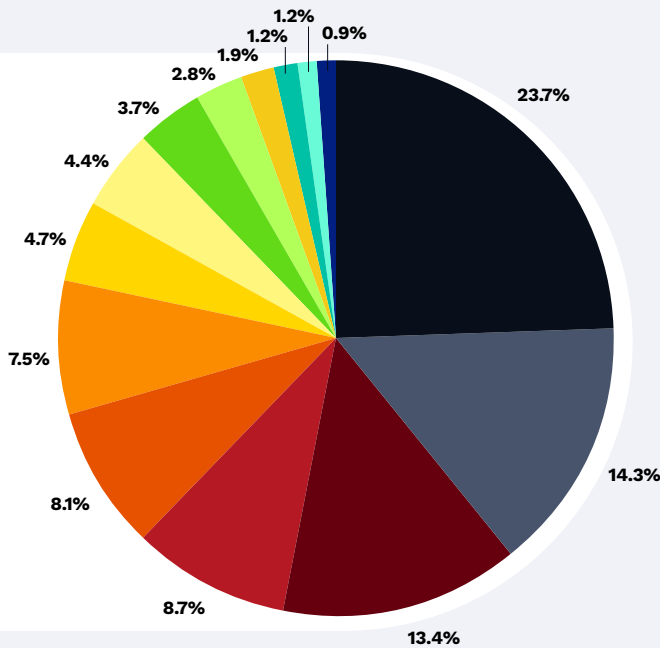
Most Commonly Risk Accepted

52%	Intel Active Management Technology 12.0.x Multiple Vulnerabilities (INTEL-SA-00241)
18.1%	Intel Active Management Technology Privilege Escalation Vulnerability (INTEL-SA-00404)
12.5%	Lexmark Printer Multiple Vulnerabilities (TE920)
5.6%	Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Windows
3.1%	Microsoft SQL Server Unsupported Version Detection
2.2%	OS End Of Life Detection
1.9%	Atlassian Jira Multiple Vulnerabilities
1.6%	MariaDB End Of Life Detection (Windows)
1.2%	jQuery End of Life (EOL) Detection
0.6%	iSpyConnect iSpy End of Life (EOL) Detection
0.6%	Oracle Access Manager (OAM) RCE Vulnerability (cpujan2022)
0.3%	Spring4Shell



High Severity:
















Most Commonly Risk Accepted



23.7%	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
14.3%	Intel Active Management Technology Multiple Vulnerabilities
13.4%	Intel Active Management Technology Multiple Buffer Overflow Vulnerabilities
8.7%	Atlassian Jira Multiple Vulnerabilities
8.1%	Apache HTTP Server Multiple Vulnerabilities
7.5%	Database Open Access Vulnerability
4.7%	Microsoft Defender Antimalware Platform Elevation of Privilege Vulnerability
4.4%	MariaDB Multiple Vulnerabilities
3.7%	SNMP Agent Default Community Names
2.8%	Lexmark Printer SNMP DoS Vulnerability
1.9%	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability
1.2%	Eclipse Jetty Multiple Vulnerabilities
1.2%	Microsoft Malware Protection Engine on Windows Defender Multiple Remote Code Execution Vulnerabilities
0.9%	Microsoft SQL Server RCE Vulnerability

CISA KEV

554 vulnerabilities were added to the CISA KEV as of **December 2022**, including:

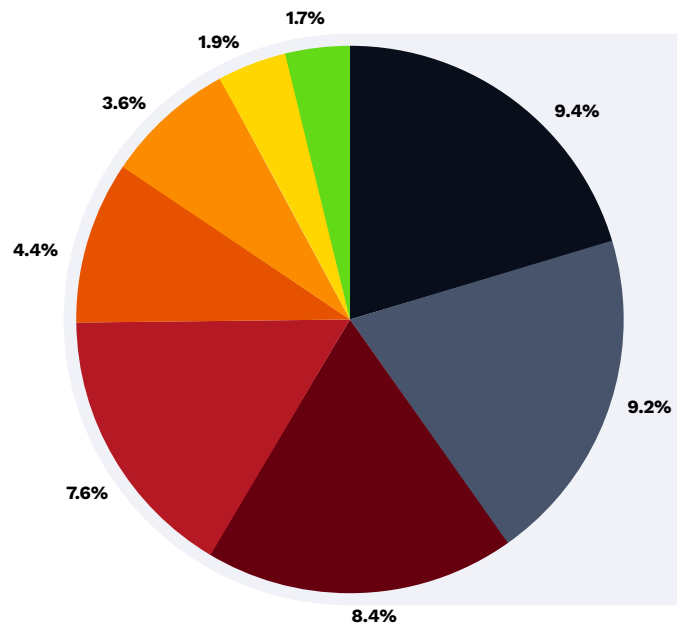
	Microsoft.....	165 additions
	Adobe.....	54 additions
	Cisco.....	50 additions
	Apple.....	25 additions
	Oracle.....	22 additions
	Google.....	21 additions
	Apache.....	13 additions
	QNAP.....	12 additions
	D-link.....	12 additions
	Vmware.....	12 additions
	Linux.....	8 additions
	Mozilla.....	7 additions
	Netgear.....	7 additions
	Zimbra.....	6 additions
	Atlassian.....	5 additions
	Citrix.....	5 additions
	Fortinet.....	5 additions
	Android.....	3 additions

Microsoft CVE 2021-1647 was the most common vulnerability discovered in 2022 which is listed on the CISA KEV.

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1647>

CISA KEV

The most common vulnerabilities discovered last year by Edgescan across over 250+ organisations and 30 industry verticals. These are listed on the CISA (Cybersecurity & Infrastructure Security Agency) KEV (Known Exploitable Vulnerability) Catalogue. CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. CISA strongly recommends all organizations review and monitor the KEV catalogue and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors. Edgescan highlights vulnerabilities which are listed in the CISA KEV to help with prioritization.



	Name	CVE
9.4%	Microsoft Windows Defender Antimalware Platform Remote Code Execution Vulnerability	CVE-2021-1647
9.2%	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability (Follina)	CVE-2022-30190
8.4%	SUSE: Security Advisory (SUSE-SU-2019:2949-1)(SUSE-SU-2020:1272-1)(SUSE-SU-2020:2721-1) (SUSE-SU-2020:2998-1) (SUSE-SU-2021:0226-1) (SUSE-SU-2021:1273-1)(SUSE-SU-2022:0189-1) (SUSE-SU-2022:0762-1)	CVE-2020-1927,CVE-2020-1934,CVE-2020-1938,CVE-2020-1472,CVE-2020-15999
7.6%	Google Chrome Security Update (stable-channel-update-for-desktop_11-2020-11)	CVE-2020-16013,CVE-2020-16017
4.4%	Sudo Heap-Based Buffer Overflow Vulnerability (Baron Samedit)	CVE-2021-3156
3.6%	Oracle Java SE Java Runtime Environment Multiple Vulnerabilities	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, CVE-2012-0507
1.9%	Adobe Flash Player Multiple Vulnerabilities - 01 Apr15	CVE-2012-4163,CVE-2012-4164,CVE-2012-4165,CVE-2012-4166,CVE-2012-4167,CVE-2012-4168,CVE-2012-4171,CVE-2012-5054
1.7%	Microsoft Malware Protection Engine on Windows Defender Multiple Vulnerabilities	CVE-2021-1647, CVE-2018-4877,CVE-2018-4878, CVE-2017-8535,CVE-2017-8536,CVE-2017-8537,CVE-2017-8538,CVE-2017-8539,CVE-2017-8540,CVE-2017-8541,CVE-2017-8542

*Percentage of total CISA KEV listed vulnerabilities discovered in 2022.

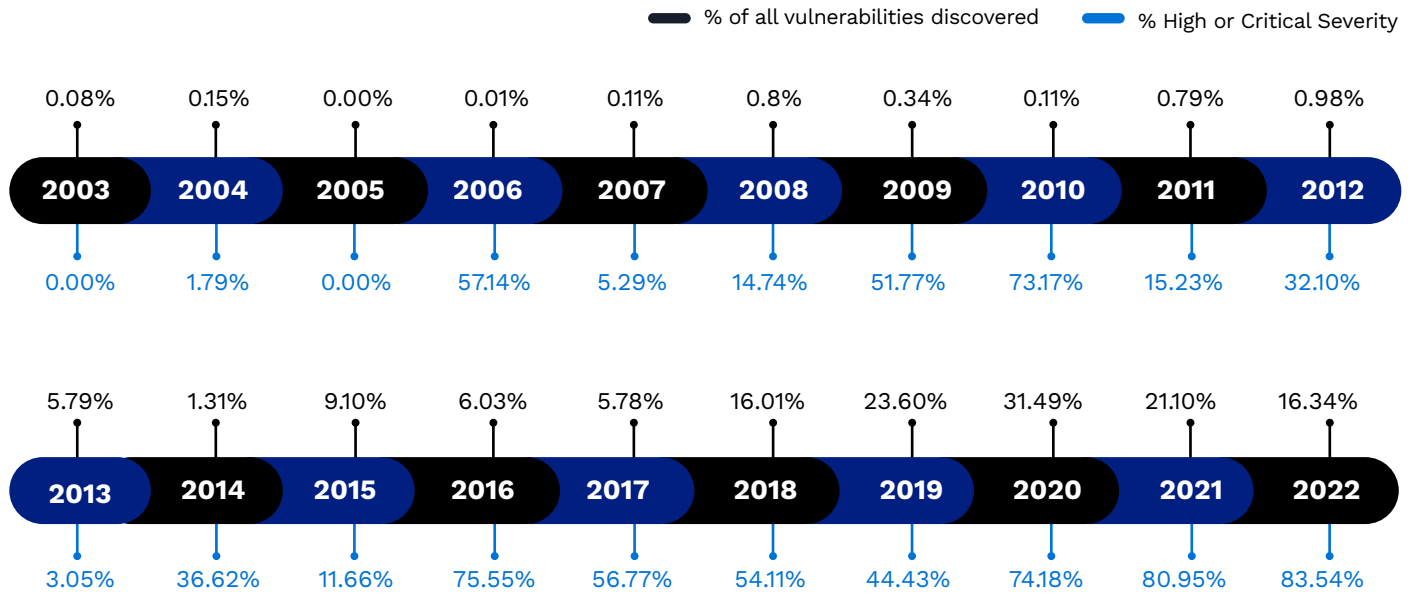
Edgescan automatically maps any discovered vulnerabilities to the CISA KEV & EPSS to aid prioritization decisions.



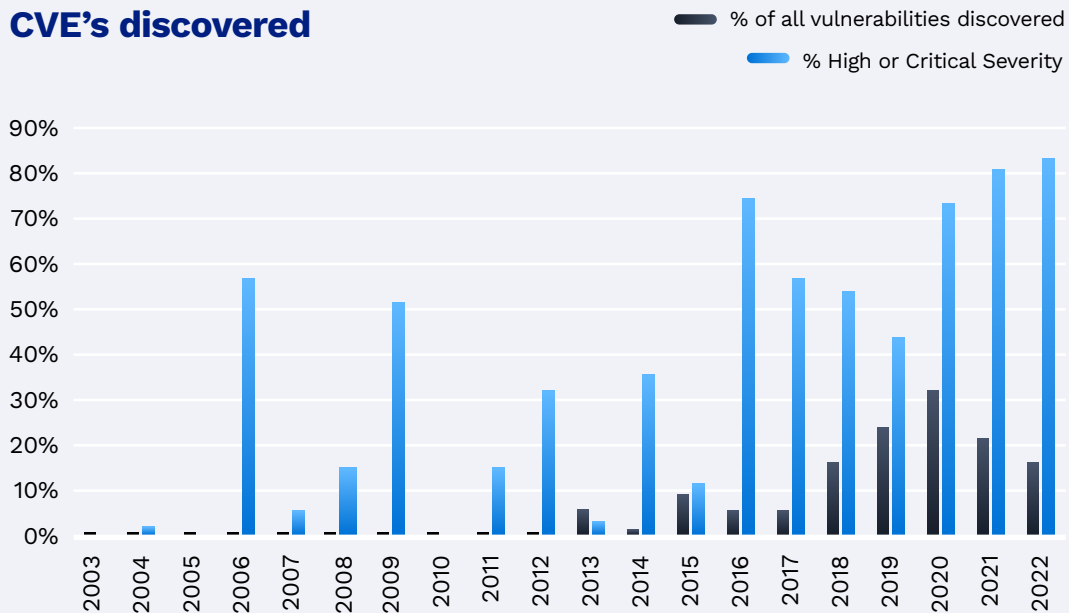
Vulnerability Age

Here we take a look at the age of all vulnerabilities discovered from **2003** to **2022**. Each vulnerability can contain more than one CVE from multiple years.

For example, **16.34%** of vulnerabilities discovered in **2022** contained a CVE from **2022**. **83.54%** of the CVE's discovered in **2022** are considered **High** or **Critical Severity**.



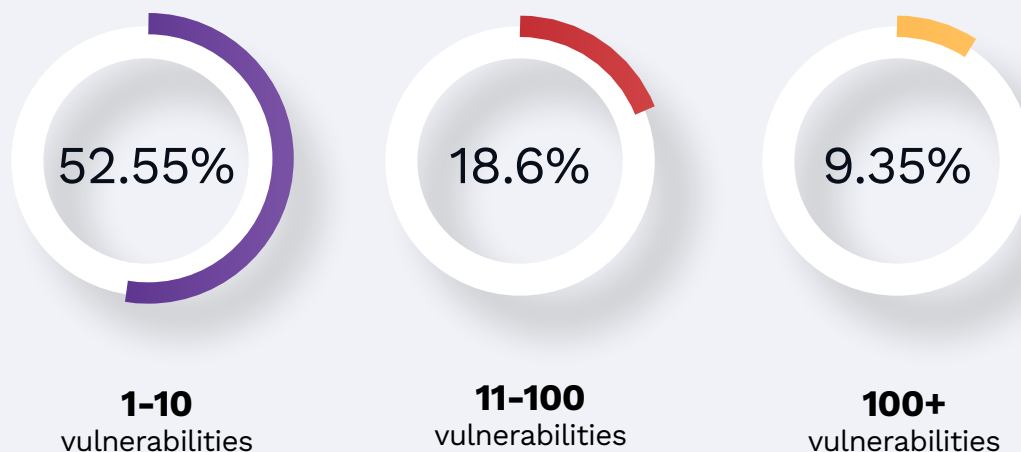
CVE's discovered



During 2022 we can see the percentages of aged CVE's discovered. E.g. 21.1% of the vulnerabilities discovered contained a CVE's from 2021 with 80% of the CVE's considered High or Critical Severity.

Vulnerability Clustering

Metrics relating to the average amount of vulnerabilities per asset. Most assets across the full stack have multiple vulnerabilities.



Above we can see:

- **52.22%** of all assets assessed in 2022 had between **1 and 10** vulnerabilities throughout the **12 month** period.
- **18.6%** of all assets assessed in **2022** had between **11 and 100** vulnerabilities & **9.35%** of assets had **100+ vulnerabilities**.

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

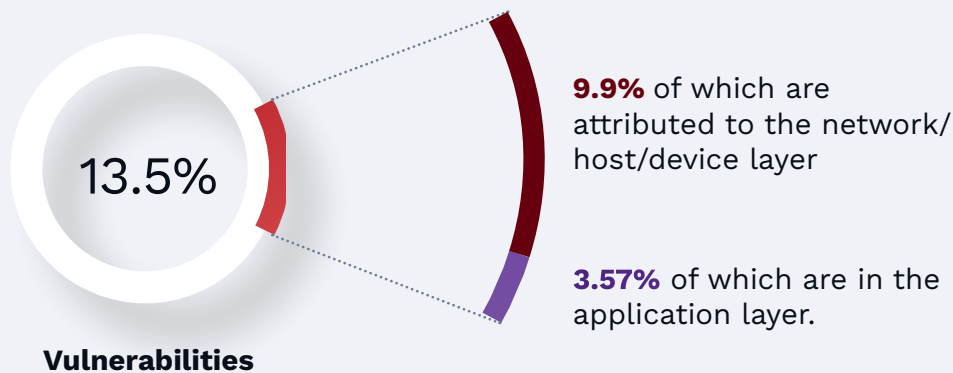
Vulnerability Backlog

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

For larger enterprises (1000+ employees), on average 41% of vulnerabilities discovered in a 12 month period remain open, they have not been remediated.

- **13.5% of vulnerabilities** in an enterprise's backlog are either high or critical severity.
- **9.9%** of which are attributed to the network/host/device layer.
- **3.57%** of which are in the application layer.

We appear to close web application and API vulnerabilities more consistently, given the majority of high and critical severity vulnerabilities on average in a vulnerability backlog reside in the network/host/device layer.



In reality there is nothing wrong with having open vulnerabilities for a long time. A cornerstone of good vulnerability management is to remediate what matters, not all vulnerabilities.

Conclusions



- ☞ We are still **not** getting the **basics right**.
- ☞ In 2022 we've observed very basic vulnerabilities many of which are commonly leveraged by cybercrime.
- ☞ **Continuous** assessment, validation & prioritization will make a huge **difference** to any organizations cybersecurity posture.
- ☞ Resilience; "Internal"/Non-Internet facing vulnerability management is certainly **overlooked**, possibly the reason for the **ease of pivot** by cyber crime organisations once they breach the perimeter.
- ☞ API security is still "**the poor relation**" to web application security possibly due to **poor tooling** and **approaches** to API security assessment. API **discovery** is also an important tool to leverage and keep pace with what's deployed publicly.
- ☞ Attack Surface Management (ASM) is **not** a "Wishlist" item and aids decent vulnerability management coverage. Many exposures ASM detects are **not CVE/OWASP** related but rather due to **poor visibility**.
- ☞ Reliance on "**ShiftLeft**" 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 backlog**.



Mr. Vulnerability and Ransomware

Why 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.

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

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.



Edgescan Reviews

Customer First

by Edgescan in Application Security Testing

4.7 ★★★★★ 44 Ratings

Certified security analysts. Battle-hardened experts

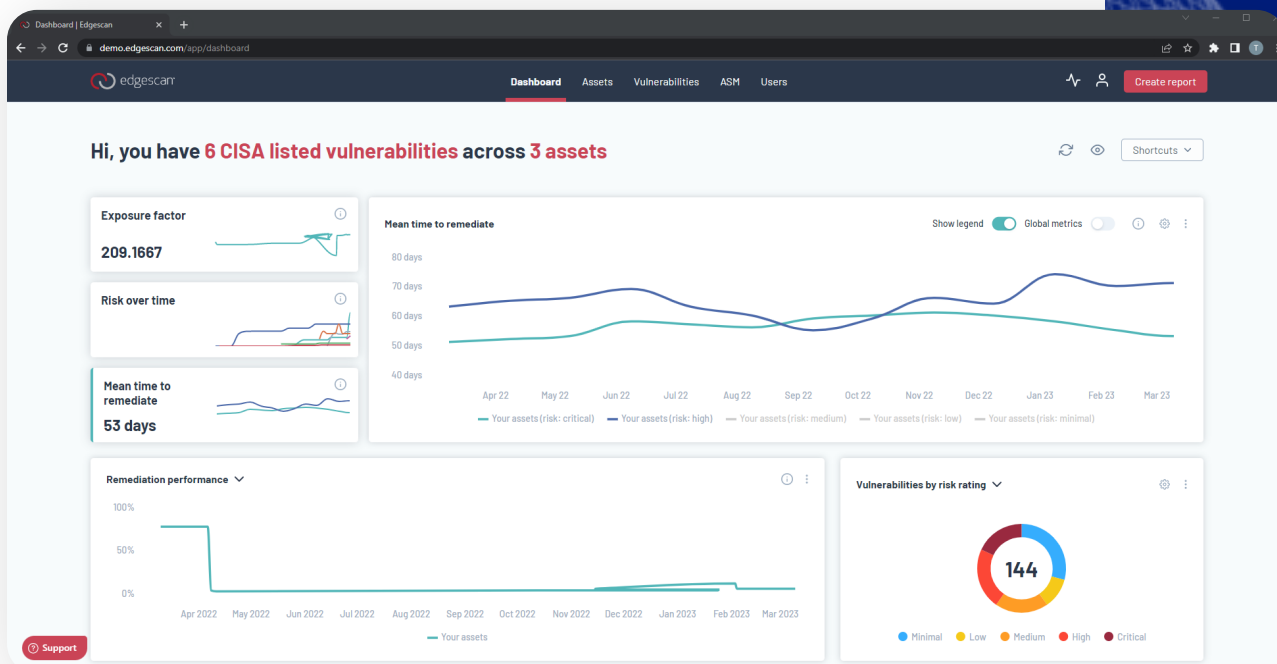
Edgescan is an ISO27001 and CREST certified organization, and our security analysts are seasoned experts and carry a range of industry credentials including CREST, OSCP and CEH certifications.

One Yearly Fee. Unlimited Access. Unlimited tests

Since Edgescan is a fixed subscription investment service we help operationalize your costs as there are no additional fees associated outside of the contract service time. In addition, Edgescan's customer support team and technical experts act as an extension of your team providing premium 24x7x365 support. The platform's automated scanning supports unlimited rescans and vulnerability retesting requiring less client resources needed to effectively manage the platform while enabling faster remediation times.

One Platform. Five Full-Featured Solutions

The Edgescan platform features five security solutions so customers can choose what works best with their existing CI/CD pipelines and current tools stack. The platform provides a unique view of risk-rated and verified vulnerability intelligence to help prioritize remediation all reviewed by the eyes of our security analysts.



Solutions Include



Penetration Testing as a Service (PTaaS)

Hybrid approach that combines the breadth of automation with the depth of human assessment.



Vulnerability Management

Full-stack coverage that automatically provides risk-rated and validated vulnerability data that is verified by certified security analysts.



External Attack Surface Management (EASM)

Continuously scours and maps your global IT ecosystem to identify security blind spots and attacker-exposed assets.



Web Application Security Testing (DAST)

Inspects every web application, host infrastructure and cloud resource looking for exposures.



API Security Testing

Identifies and probes active endpoints and then proactively monitors network changes.

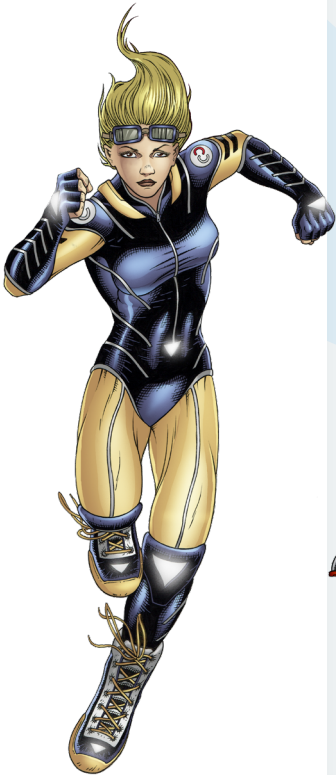
Stronger Together.

The Edgescan Universe

Security pros must be ever vigilant to safeguard their data and The Edgescan Universe cast of heroes is a representation on how we perceive our staff, our customers, our partners... and all security pros. Check out our website to see our lineup of heroes... and the villains they fight.

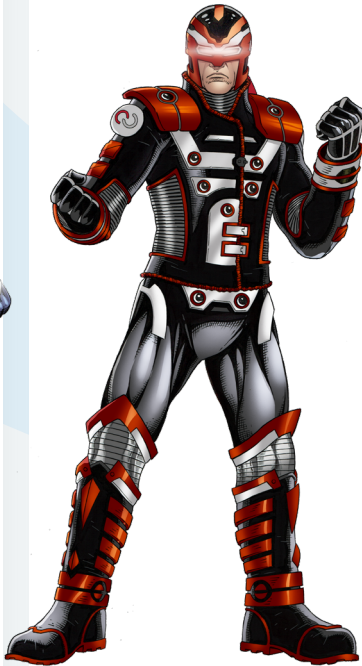


Infinity



Assessment on an infinite scale.
Never gets tired.

Mapper



Continuous vigilance across the battlefield.
Identifies the attack surface to protect.

Scale



Nothing too big for scale. Scale supports accuracy.

Validator



She never makes mistakes.
Identifies real risks and helps the team focus on what matters.

Glossary

Asset	A web application, an IP network range, mobile application, API, microservice or a CI/CD pipeline
API	Application Programming Interface
CI/CD	Continuous Integration / Continuous Deployment
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DNS	Domain Name System
DOM	Document Object Model
External	Public Internet Facing
FTP	File Transfer Protocol
Internal	Non-Public Internet Facing
MTTR	Mean Time To Respond/Remediate
PCI	Payment Card Industry
PTaaS	Penetration Testing as a Service
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SME	Small and Medium Enterprises
SSH	Secure Shell
SSO	Single Sign-On
XML	Extensible Markup Language
XSS	Cross-Site Scripting



Illuminate & Eliminate Cyber Risk

US: +1 332 245 3220

UK: +44 (0) 20 3855 5592

IRL: +353 (0) 1 6815330

Sales and general enquires:

sales@edgescan.com

edgescan.com

