edgescan™

2021
VULNERABILITY STATISTICS REPORT

edgescan.com

Table of contents

Introduction 3

2020. Year in review 5

Risk Density 7

Risk Density by organization size 8

Application Security 9

Fullstack Vulnerability View. Critical Risks 2020 12

Mean Time to Remediate (MTTR) 13

MTTR based on company size 14

Most common Risk-Accepted Vulnerability 15

CVE - Landscape 16

Top CWE Common Weakness Enumeration 2020 22

Malware, Ransomware and CVE's 23

CVE Dispersion and Clustering 25

Exposed – Services and Ports 26

Edgescan Heroes and Villains 27

About Edgescan 28

Glossary 30

Introduction

For our 6th Year running, welcome to the Edgescan Vulnerability Stats Report.

This report aims to demonstrate the state of full stack security based on thousands of security assessments performed globally, as delivered by the Edgescan SaaS during 2020.

I am still as passionate as ever in compiling this report and delving into the underlying data, as it gives unique insight into what's going on from a trends and statistics perspective and indeed a snapshot of the overall state of cyber security.

The Edgescan report has become a reliable source for truly representing the global state of cyber security vulnerability management. This is becoming more evident as our unique dataset is now also part of other annual security analysis reports, such as the OWASP Top 10 and Verizon DBIR (we are happy contributors for many years now).

This year we took a deeper look at vulnerability metrics from a known vulnerability (CVE), Malware, Ransomware and visibility standpoint (exposed services), coupling both internal and public Internet-facing systems.

We still see high rates of known (i.e. patchable) vulnerabilities which have working exploits in the wild, used by known nation state and cyber criminal groups. So yes, patching and maintenance is still a challenge, demonstrating that it is not trivial to patch production systems.

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

The web application layer is where the majority of risk still resides, but some lower layer (Host/Operating system/Protocol) issues, if discovered, could also present headaches if exploited. CVE's as old as 2015 are being used by ransomware and malware toolkits to exploit systems within "the perimeter".

Visibility is a key driver to cyber security and based on our continuous asset profiling we discuss how common sensitive and critical systems are exposed to the public Internet. For example we saw in increase by 40% of exposed remote desktop services due to the increase in remote working during the year. The assumption here is that enterprises simply did not have the visibility or systems in place, to make them aware of, or inform them of the exposure.

Similar to last years report, we also delve into "internal" cyber security, looking at metrics which may not seem as important, but are a valuable defense in the case of malware infection, ransomware and other internal attacks.

Such malware, ransomware and APT actors leverage common vulnerabilities in corporate networks to spread across the enterprise. This report provides a glimpse of a global snapshot across dozens of industry verticals and how to prioritize on what is important, as not all vulnerabilities are equal. This year we call out which threat actors are leveraging discovered vulnerabilities, which should be food for thought.

Best regards,

Eoin Keary

“The web application layer is where the majority of risk still resides....CVE’s as old as 2015 are being used by ransomware and malware toolkits to exploit systems within “the perimeter“....”

SCALE

Nothing is too big for scale. Scale supports accuracy and coverage.

2020. Year in review

2020 was an unprecedented and tough year for most. It is with some optimism that we face into 2021 although certain new norms, such as widespread remote working, will remain a key part of the future workplace. The following discusses a number of newsworthy items relating to cyber security, exposures and items relating to the Edgescan vulnerability statistics, to follow.

Mass remote working has resulted in a major change to how businesses work and how people connect to their workplaces. The Covid-19 pandemic has seen a large increase in remote working but also a significant increase in attack surface in 2020. **We observed an increase of exposed/insecure Remote Desktop Services by 40%.**

SolarWinds/Supply Chain attacks: one of the largest attacks in history with over 250 USA government agencies and many global businesses being affected. The supply chain attack is insidious by exploiting a single point, resulting in malicious code being distributed to all organizations using the update mechanism.

Edgescan won multiple Industry & Service Delivery awards, many of which were by public vote (thanks - we appreciate the love!). We won the **Penetration Testing Solution of the year 2020 (Computing Security Awards), Cloud-Delivered Security Solution of the Year 2020 (Computing Security Awards), Best Vulnerability Management Solution (SC Awards Europe 2020) and Best Enterprise Security Solution - Highly Commended (SC Awards Europe 2020)**. Overall we were delighted that our hard work paid off in such a strange and difficult year. We were also delighted to win a design award for our new user interface - the **"Good Design Award 2020"** ↗.

Gartner Peer Insights. We are still one of the highest scoring Application Security Testing solutions in peer insights! It is humbling as always to receive such a high number of brilliant reviews on our solution ↗.

Increase End-user attacks: With "everyone" working remotely, attackers have focused on the end user now more than ever. Phishing attacks, Ransomware, Data theft are all increasing. Many Ransomware and malware attacks are a result of exploitation of CVE's (Known vulnerabilities). Remote working makes an attackers life easier due to it being more difficult to maintain and update remote workers devices.

Increase in online commerce & attacks. More and more businesses are delivering e-commerce solutions due to the "high street" not being as available as a result of the pandemic. The rush to "go-online" by businesses has resulted in more vulnerabilities and an uptick in insecure systems and data theft.

Ransomware increases as a result of end-user attacks. Coupled with phishing attacks, ransomware has risen by nearly 50% in 2020 to circa $20 billion, compared to $11.5 billion in 2019 and $8 billion IN 2018. Many of the active exploit toolkits used by cyber criminals are leveraging CVE's from 2017-2019. The most common CVE discovered in 2020, used by cybercrime actors, was CVE-2019-0708 which is used by "Bluekeep" variants.

Magecart is still growing: a supply chain attack which is exploited by a hacker substituting a piece of JavaScript code, or by redirecting shopping carts using an injection to a website that hosts the malware. We are seeing an increase in such attacks.

2020 Computing Security Awards WINNER Penetration Testing Solution of the Year

2020 Computing Security Awards WINNER Cloud-Delivered Security Solution of Year

SC Awards 2020 EUROPE highly commended Best Enterprise Security Solution

SC Awards 2020 EUROPE WINNER Best Vulnerability Management Solution

2019 Tech EXCELLENCE AWARDS WINNER MSSP OF THE YEAR

Struggling With Visibility

In general we see that organisations struggle with visibility of their own IT estates, knowing what is running and where, at any given time. This can and likely has lead to many security breaches, some of which were hot topics during the year.

Breaches of note:

- **Marriot Data breach** (5.2 million guests data) via stolen credentials; It is understood the credentials were obtained via credential stuffing and phishing attacks.
- **Travelex services** were shut down following a malware infection due to exploitation of known vulnerabilities (CVE). The company and associated businesses using the platform to provide currency exchange services, were all affected. Continuous assessment and maintenance can make a company more resilient to such attacks.
- **Microsoft** disclosed that five servers used to store user analytics were exposed and open on the Internet without adequate protection. This was due to the lack of visibility of systems in production. Again, continuous asset profiling would prevent this.
- **Virgin Media** suffered an exposure of 900,000 users through an open marketing database. This was due to an exposed database/system. Again, continuous asset profiling would prevent this.
- **MCAWizard** where a chat App for corporate funding was linked to an exposed database, resulting in 425GB of company and client data being stolen. The root cause was understood to be an exposed database. Continuous asset profiling would have helped prevent this one too!
- **EasyJet:** Mass theft of customer data, 9,000,000 customers records. It was claimed that the attack was highly sophisticated. 2,208 credit card details including the CVV data was compromised. EasyJet shouldn't be storing card CVV details, in order to be compliant with PCI standards. It is suspected that the attack was a Magecart style attack which is exploited by altering the code on the website.

> *"...the Edgescan vulnerability stats report provides us with guidance on what to focus on for the coming year and where to use our limited resources..."*

Risk Density

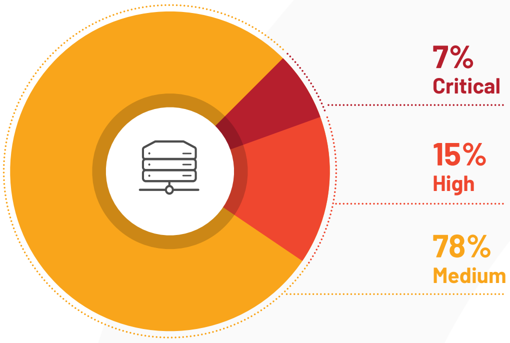
Rate of occurrence of vulnerabilities as a percentage of all vulnerabilities discovered. The detail below covers both "External" (public Internet-facing) and "Internal" (non-public facing) systems across both web applications and infrastructure layers (Full stack).

Edgescan depicts risk via the typical "Info/Low/Medium/High" risk nomenclature (similar to the OWASP Risk Rating Methodology) and also via CVSS Score. CVSS scores may not always be accurate due to not taking the context of a vulnerability into account.

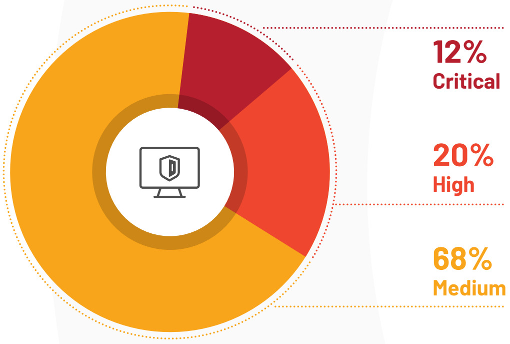
Rating Ratings	CVSS Score
Low Risk	0.1 - 3.9
Medium Risk	4.0 - 6.9
High Risk	7.0 - 8.9
Critical risk	9.0 - 10.0

External facing

Host/Network Layer



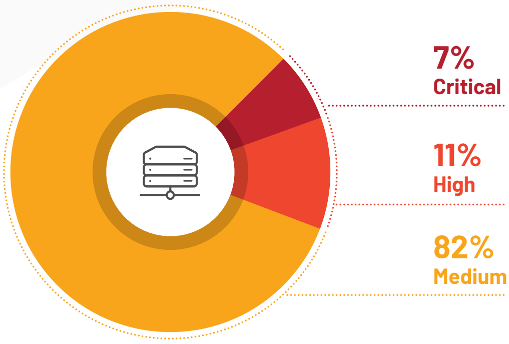
Application Layer



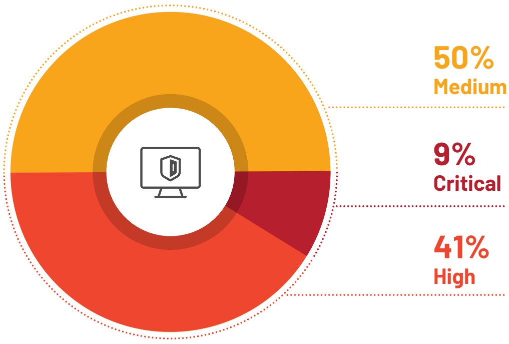
Internet facing web applications still have a significantly higher Risk Density, with 32% of vulnerabilities discovered rated as High or Critical Risk, compared to Internet facing network / Host systems, with a High or Critical risk density of 21%.

Internal facing

Host/Network Layer



Application Layer

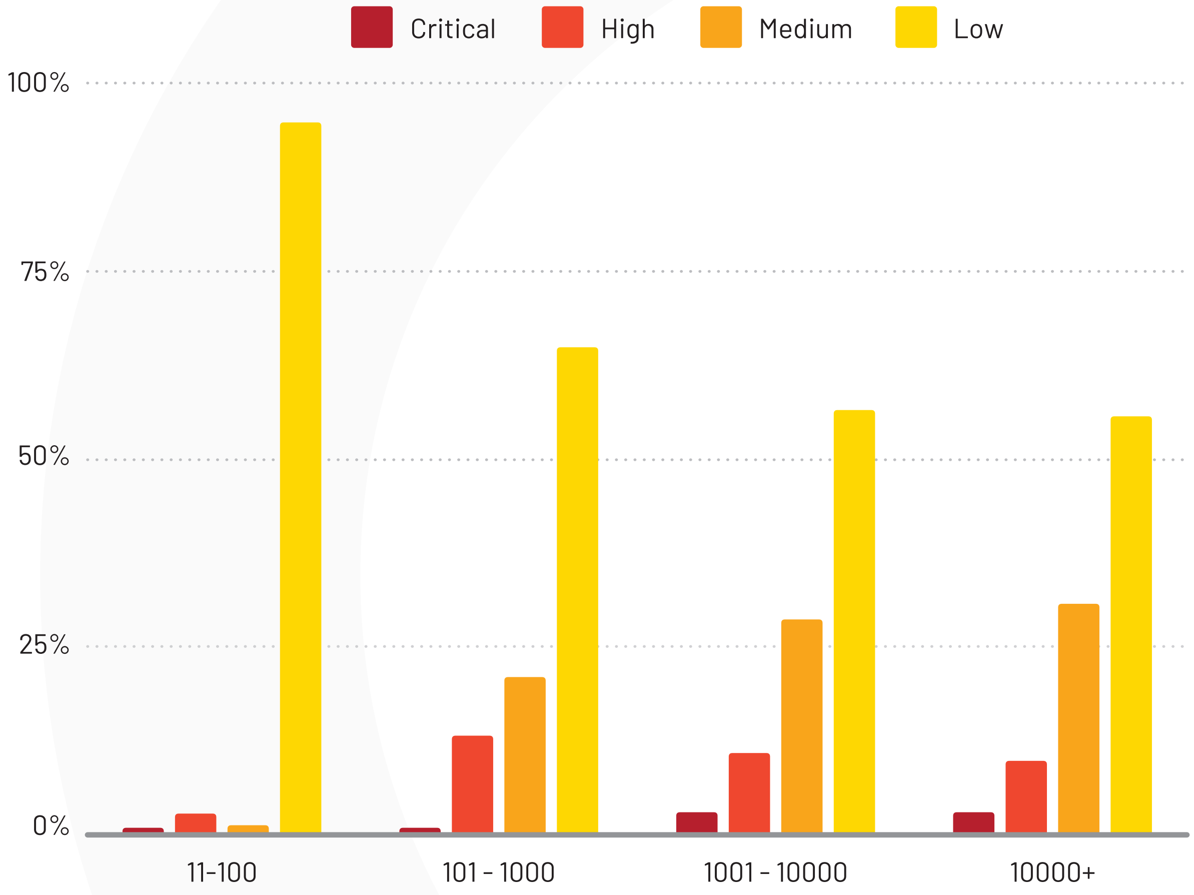


Risk Density by organization size

We analyzed risk density when applied to the size of an organization, from SME's to large enterprises.
For small organizations (with 11-100 staff) we can see the combined Medium + High + Critical Risk % of all vulnerabilities is **5%**.

This is likely due to such organizations simply having a smaller digital estate and thus attack surface.

In our experience we see **an slight increase in the occurrence of critical and high risk issues for larger organisations**. We believe this is probably due to a much larger estate to secure and relatively less people (lower ratio of staff size to security expertise) to deliver.



Application Security

Critical Risk Top 10

Definition of a Critical Risk Vulnerability: "Exploitation of the vulnerability likely results in complete compromise of services or data. Exploitation is relatively trivial in the sense that the attacker does not need any special authentication credentials or knowledge about the system to initially exploit a system. Likelihood of exploitation is generally very high"

The Application Security **Critical Risk Top 10** depicts the most common critical risk issues discovered by Edgescan in **2020**.

SQL Injection is still the main contender which is interesting to note as we can easily develop code which is not vulnerable to such attacks.

Something which is overlooked quite frequently is malicious file uploads. This can give rise to ransomware, malware and internal network breach pivot points for attackers.

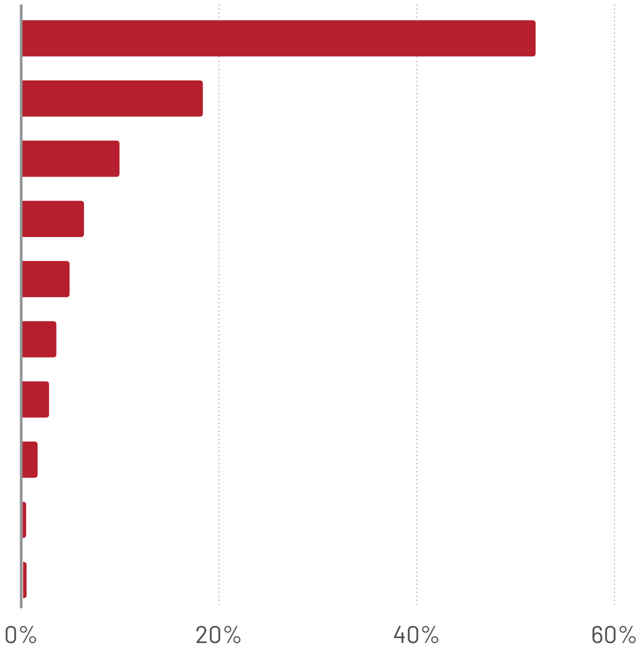
Executable code injection is commonly used by exploit kits to get access to data and source code of a system. The root cause is due to a system interpreting data as code and executing it.

Sensitive Interface or exposed data relates to the exposure of an administration control panel which could result in system breach.

An example of **data exposure** when referring to critical risks is client data, sensitive configuration information, exposed **authentication** credentials or other data which may lead to a system breach.

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

Critical Risk Issues	% of occurrence
SQL Injection	51.70%
Cross-site scripting (stored)	18.20%
Malicious File Upload	9.80%
Executable Code injection / Web Shell	6.30%
Sensitive Interface or data Exposed	4.90%
Framework Unsupported Version Detection	3.50%
Authorisation Issue	2.80%
Information disclosure	1.40%
Blind SQL Injection	0.70%
File path traversal	0.70%



Application Security

High Risk Top 10

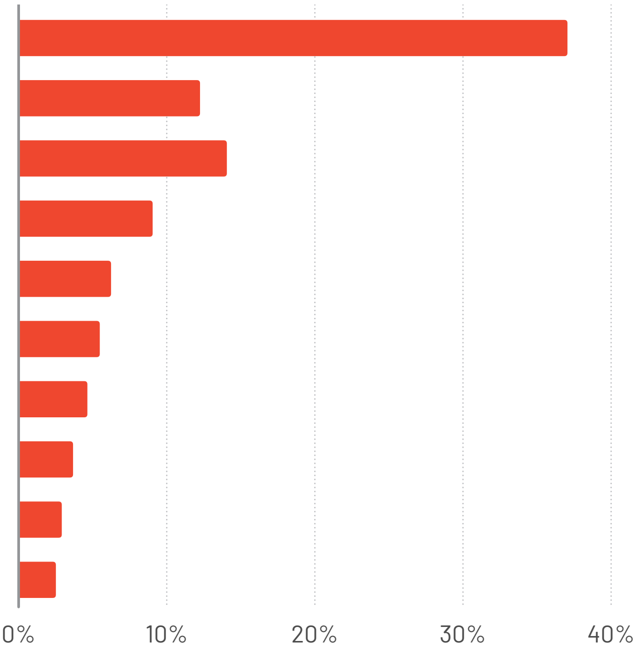
> *Definition of a High Risk Vulnerability: "Exploitation of the vulnerability likely results in significant compromise of services or data. Exploitation takes expertise in the sense that the attacker may need to be experienced. Likelihood of exploitation is generally high."*

Our old friend **Cross-Site Scripting (XSS)** (37.2%) is still king of the hill for High risk issues. This can be used for **phishing attacks**, redirection to malicious sites, malware proliferation, but to name a few. Think of XSS as a **payload** delivery vulnerability.

Exposed Administrative interfaces (9.2%) are easy to fix once you know about them. Visibility is king as we cant fix what we don't know about. – *Say "hello" to continuous asset profiling!*

XML external entity injection (4.7%) (also known as XXE) is a vulnerability that allows an attacker to manipulate an applications processing of XML data. It can allow an attacker to do things such as gain **unauthorized access** to files on the application server filesystem, or interact with downstream back-end or external systems that the application itself can access, by virtue of injecting specific payloads. In the case of high risks, the XXE in question resulted in **system compromise** and data exfiltration.

High Risk Issues	% of occurrence
Cross-Site Scripting - XSS (reflected/ DOM)	37.20%
Brute Forcing & Weak Authentication	12.40%
File path traversal	14.20%
Administrative Interface Exposed	9.20%
Framework Deprecated Version	6.20%
Information Disclosure	5.50%
XML external entity injection	4.70%
No cryptography	3.70%
Server Side Request Forgery	3.00%
Authorization Issue	2.50%



Application Security

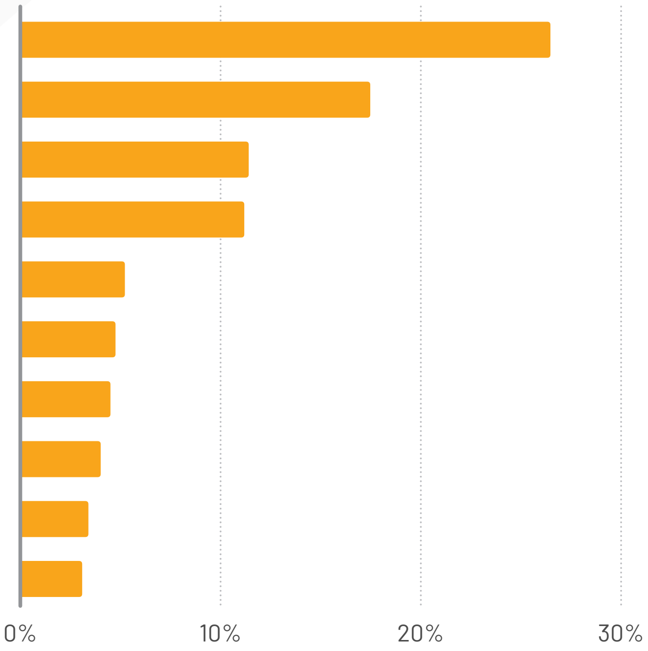
Medium Risk Top 10

> *Definition of a Medium Risk Vulnerability: "Exploitation of the vulnerability likely results in limited compromise of services or data. Exploitation may require user privileges or additional social engineering to be successful. Likelihood of exploitation is generally medium."*

Weak authentication (26.5%) can be a difficult fix when user experience and low friction application access is important. It is certainly worth considering **Multi-factor authentication** for higher privileged accounts or when committing a valuable transaction. Single Sign-On (SSO) should also be considered.

Exposed sensitive services (5.3%) can result in catastrophic exploitation and are **trivial** to mitigate. Itis highly recommended to invest time and search for such things.

Medium Risk Issues	% of occurrence
Cross-Site Scripting - XSS (reflected/ DOM)	37.20%
Brute Forcing & Weak Authentication	12.40%
File path traversal	14.20%
Administrative Interface Exposed	9.20%
Framework Deprecated Version	6.20%
Information Disclosure	5.50%
XML external entity injection	4.70%
No cryptography	3.70%
Server Side Request Forgery	3.00%
Authorization Issue	2.50%



Fullstack Vulnerability View. Critical Risks 2020

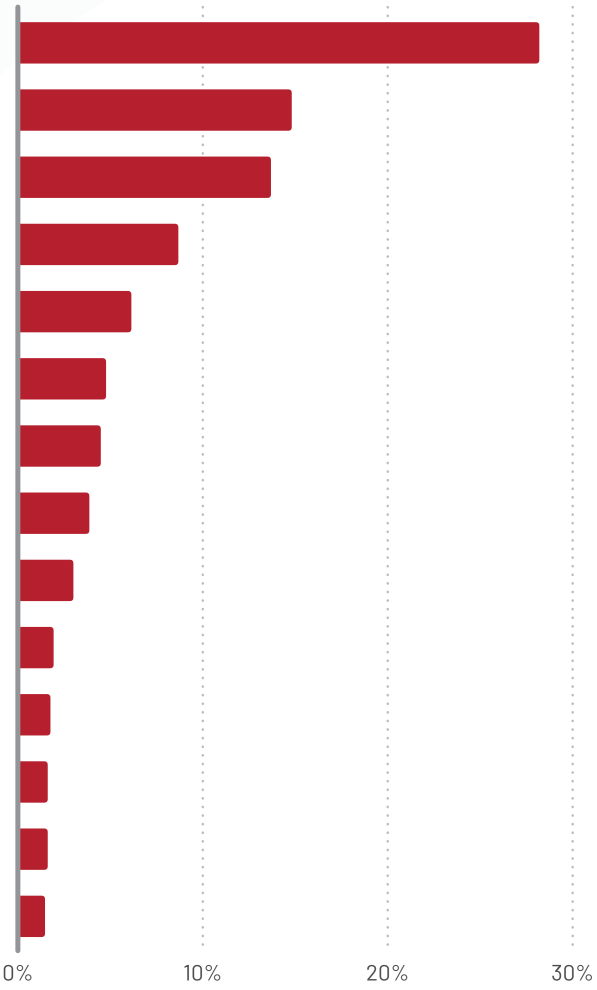
Most common critical vulnerabilities across the full stack.

Looking at vulnerabilities from a pure risk standpoint is interesting as we delve into what types of vulnerabilities are being discovered, be them technical, logical, patching-related or coding as the root cause. The following is a high level breakdown of **the most common critical vulnerabilities discovered and validated in 2020** by the Edgescan™ SaaS.

Obviously there are thousands of different vulnerability types discovered in a 12 month period but below are some of the more interesting and common ones...

> *"So, we got to thinking, how about we single-out the most common critical risks across the full stack and maybe, if folks focus on preventing these issues, things might improve a little..."*

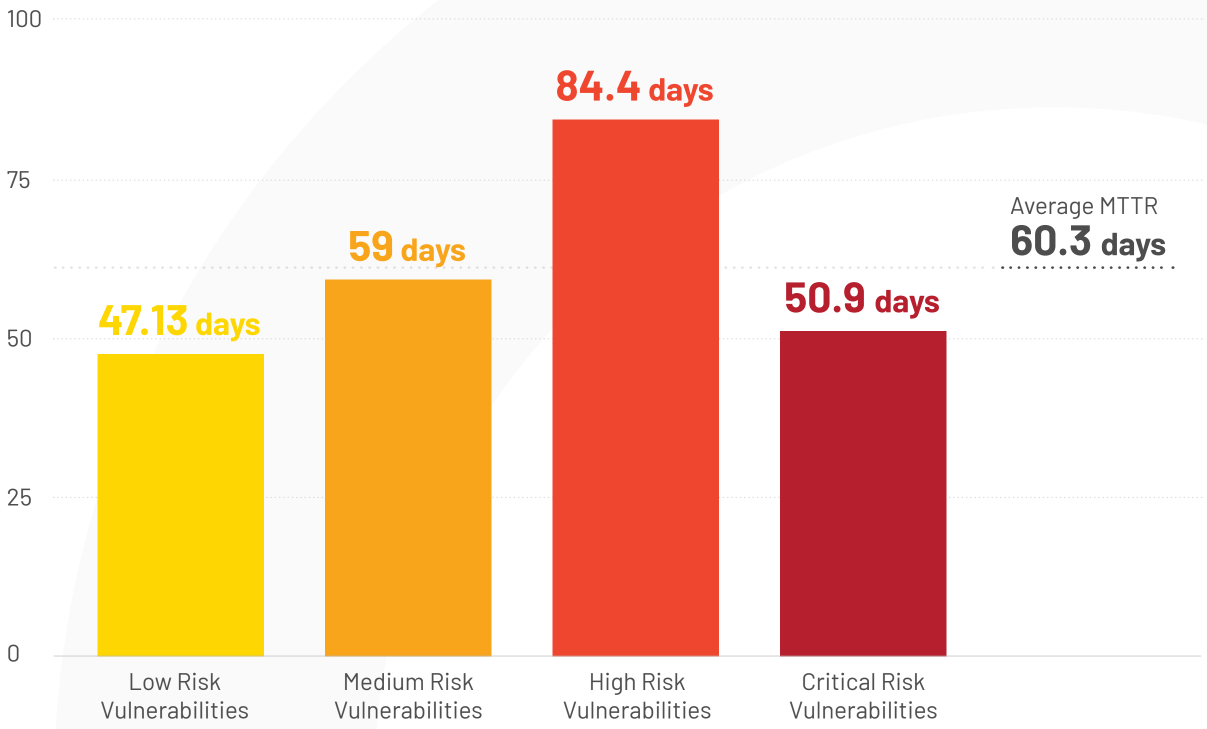
Critical Risk Issues	% of occurrence
PHP Multiple Vulnerabilities	27.4%
Oracle Weblogic Vulnerabilities	14.5%
Obsolete/End of Life system	13.4%
Remote Code Execution (RCE)	8.3%
Default/No Credentials	5.9%
SAP Message ServerSAP NetWeaver SAP RFCSAP Web GUI	4.6%
SQL Injection	4.3%
Apache Tomcat	3.7%
Apache HTTP Server	2.8%
Dell EMC/IDRAC	1.7%
Discard Service Detection	1.6%
Cross-site scripting (stored)	1.5%
Command Injection	1.4%
Authorisation Issue	1.2%



Mean Time to Remediate (MTTR)

We are still taking some time to mitigate high and critical risk vulnerabilities. In many cases high and critical risk issues can be more complex and difficult to fix but other times it can be a simple patch or system configuration tweak.

Critical Risks (on one side of the scale) and Low risk (on the other) appear to be mitigated quicker...This could be due to urgency to fix (Critical risks) coupled with ease of fix (Low Risks).



Average MTTR for Web Application Vulnerabilities: **50.3 Days**

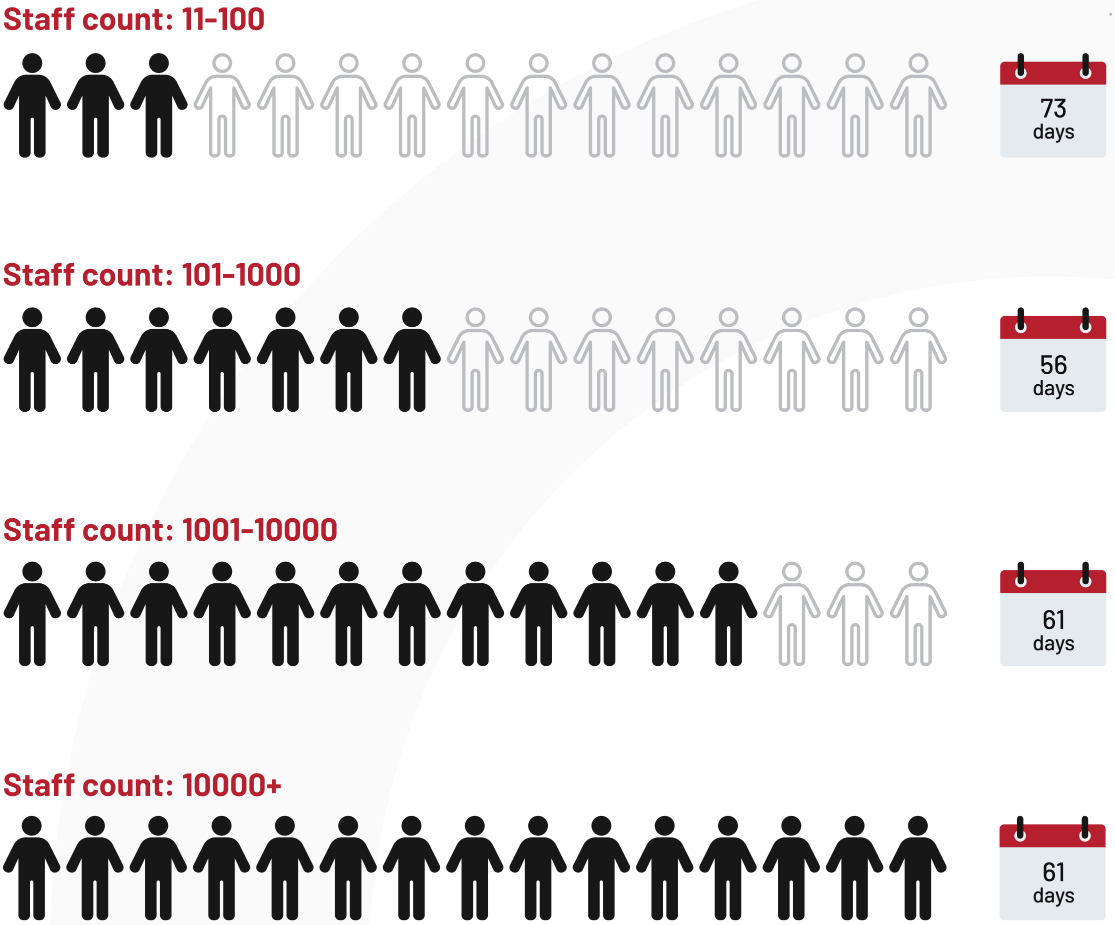
Average MTTR for Host/Network Vulnerabilities: **63.1 Days**

Quickest Mitigation time – Host/Network: **1hr 45mins**

Slowest Mitigation time: **309 Days**

MTTR based on company size

It appears that company size generally has little or no impact in relation to the time it takes to fix vulnerabilities. We measured time-to-fix of critical risk vulnerabilities for a number of company sizes and the average is much the same across the various samples.



- We believe the size of an organization does not impact speed of security.
- IT and Information Security generally does not grow linearly with the size of a business.
- Larger organizations have more to secure, more data and systems, but generally not relatively more security staff!

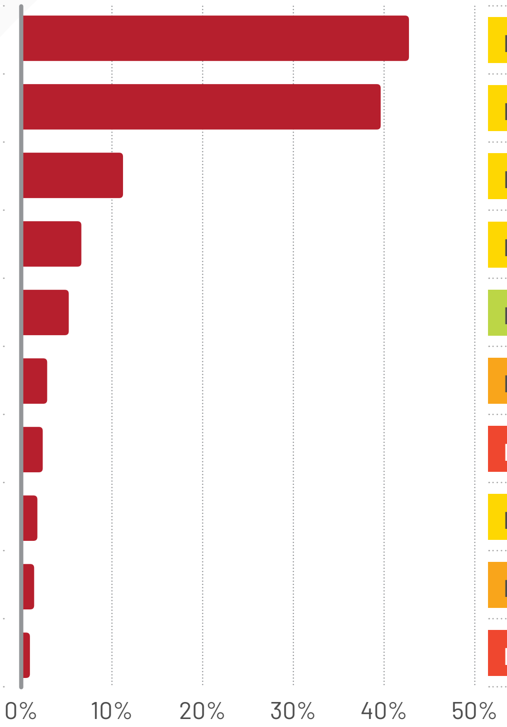
Most common Risk-Accepted Vulnerability

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 the fact that an upcoming change might remove the risk completely.

In 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 it can be tracked but it is not deemed a risk by the organization. The below table shows a list of the most common vulnerability types that our clients tend to accept the risk posed by them.

Vulnerability Type	Risk Accept rate	Risk
HTML5 cross-origin resource sharing	42.66%	Low
Frameable response (potential Clickjacking)	39.61%	Low
Cacheable HTTPS response	11.08%	Low
Cookie Security	6.66%	Low
API Endpoint discovery	5.30%	Informational
Host header poisoning	2.80%	Medium
Malicious File Upload	2.40%	Medium/High
Vulnerable Javascript library	1.90%	Low
Brute Forcing Possible	1.28%	Medium
Cross-Site Scripting - XSS (reflected)	1.10%	Medium/High



CVE - Landscape

Oldest vulnerability discovered in 2020: 21 years old (1999)

CVE-1999-0517

Default SNMP community name: An empty or missing name, akin to a password, found for a service running the SNMP network management protocol.

Base CVSS Score (2.0): 7.5 (High)

Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)

PCI: Fail

Most Common Vulnerability (CVE) discovered in 2020: Logjam

CVE-2015-4000

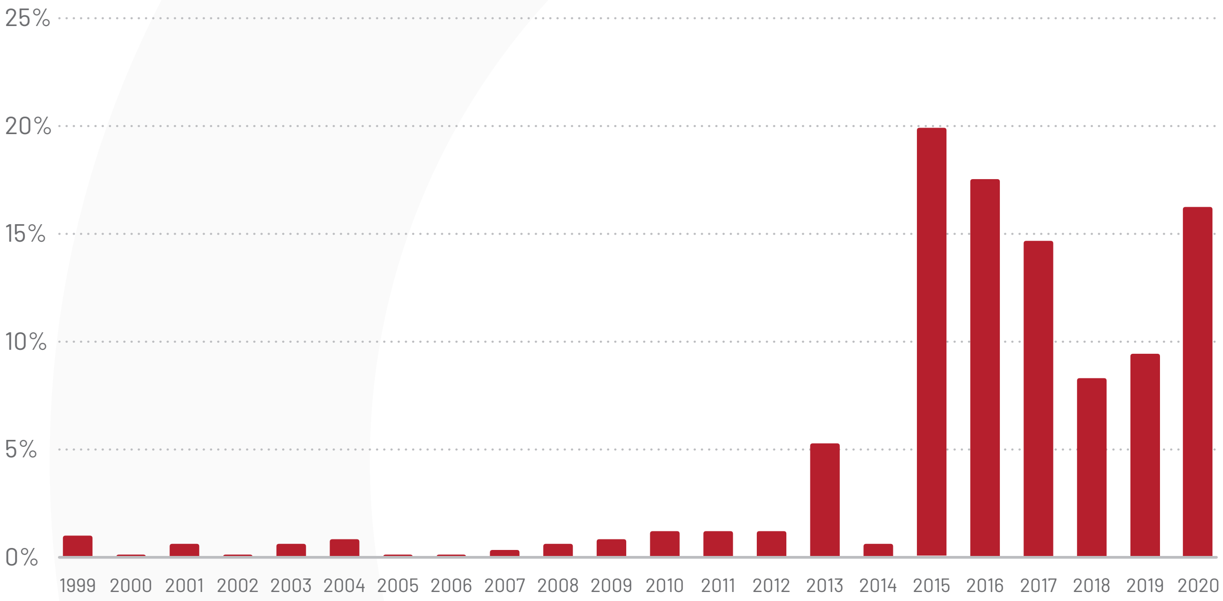
Logjam: A vulnerability with cryptosystems using Diffie-Hellman key exchanges of certain key strengths, facilitating man-in-the-middle attacks.

CVSSv2: 4.3, CVSSv3: 3.7

Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

PCI: Fail

% of all discovered CVE's



We are still finding very old "known vulnerabilities". Some of these may not be a high risk, but from our 2020 data some are actively used by cybercrime and nation state attackers.

88% of CVE's are between **0-5 years old**. CVE's from 2015 are the most common.

CVE - Landscape (all CVE's)

Most Common Critical Risk CVEs discovered in 2020 – **Score of 8.0 and above**. The Occurrence % is the rate of occurrence compared to all Critical risk vulnerabilities discovered in 2020.

CVE	CVSSv2	CVSSv3	Occurrence %
CVE-2018-0598	9.3	7.8	2.72%
CVE-2015-5600	8.5		0.97%
CVE-2019-0708	10	9.8	0.94%
CVE-2017-0143	9.3	8.1	0.86%
CVE-2017-0144	9.3	8.1	0.86%
CVE-2017-0145	9.3	8.1	0.86%
CVE-2017-0146	9.3	8.1	0.86%
CVE-2017-0148	9.3	8.1	0.86%
CVE-2019-3705	10	9.8	0.75%

CVE-2018-0598

Untrusted search path vulnerability in Self-extracting archive files created by IExpress bundled with Microsoft Windows allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.

CVE-2015-5600

The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

CVE-2019-0708

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

CVE-2017-0143

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

CVE-2019-3705

Dell EMC iDRAC6 versions prior to 2.92, iDRAC7/iDRAC8 versions prior to 2.61.60.60, and iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22 and 3.23.23.23 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to crash the webserver or execute arbitrary code on the system with privileges of the webserver by sending specially crafted input data to the affected system.

*Note all CVE descriptions used are directly referenced from the National Vulnerability Database (nvd.nist.gov)

CVE – Landscape

External Facing Assets

Most Common External facing CVE's discovered in 2020. The Occurrence % is the rate of occurrence compared to all public facing vulnerabilities discovered in 2020.

CVE	CVSSv2	CVSSv3	% occurrence
CVE-2015-4000	4.3	3.7	2.72%
CVE-2013-2566	4.3	5.9	1.93%
CVE-2015-2808	5		1.93%
CVE-2016-2183	5	7.5	1.40%
CVE-2017-5645	7.5	9.8	0.94%
CVE-2019-17571	7.5	9.8	0.71%
CVE-2013-5855	4.3		0.44%
CVE-2014-2470	7.5		0.44%
CVE-2014-2479	6.8		0.44%
CVE-2014-2480	6.8		0.44%

CVE-2015-4000

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

CVE-2013-2566

The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

CVE-2015-2808

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.

CVE-2016-2183

The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.

CVE-2017-5645

In Apache Log4j 2.x before 2.8.2, when using the TCP socket server or UDP socket server to receive serialized log events from another application, a specially crafted binary payload can be sent that, when deserialized, can execute arbitrary code.

CVE – Landscape

External Facing Assets

CVE-2019-17571
Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.

CVE-2013-5855
Oracle Mojarra 2.2.x before 2.2.6 and 2.1.x before 2.1.28 does not perform appropriate encoding when a (1) <h:outputText> tag or (2) EL expression is used after a scriptor style block, which allows remote attackers to conduct cross-site scripting (XSS) attacks via application-specific vectors.

CVE-2014-2470
Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.0.2.0, 10.3.6.0, 12.1.1.0, and 12.1.2.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS Security.

CVE-2014-2479
Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.0.2.0, 10.3.6.0, 12.1.1.0, and 12.1.2.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS - Web Services.

CVE-2014-2480
Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.0.2.0, 10.3.6.0, 12.1.1.0, and 12.1.2.0 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2014-2481.

SNAKE OIL

A joker and scoundrel. Never a true word can be said by snake oil. Loves building up your hopes only to let you down with a bang!

CVE – Landscape

Internal Facing

Most Common internal facing CVE's discovered in 2020. The Occurrence % is the rate of occurrence compared to all internal facing vulnerabilities discovered in 2020.

CVE	CVSSv2	CVSSv3	% Occurance
CVE-2015-4000	4.3	3.7	16.80%
CVE-2013-2566	4.3	5.9	13.80%
CVE-2015-2808	5		13.80%
CVE-2015-8156	7.2	7.8	8.90%
CVE-2009-2761	7.2		8.00%
CVE-2012-4350	7.2		7.70%
CVE-2013-0513	7.2		7.50%
CVE-2013-1092	7.2		7.30%
CVE-2013-1609	6.8		7.30%
CVE-2013-1610	6.8		7.20%

CVE-2015-4000

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

CVE-2013-2566

The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

CVE-2015-2808

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.

CVE-2015-8156

Unquoted Windows search path vulnerability in EEDService in Symantec Endpoint Encryption (SEE) 11.x before 11.1.1 allows local users to gain privileges via a Trojan horse executable file in the %SYSTEMDRIVE% directory, as demonstrated by program.exe.CVE-2017-5645

CVE – Landscape

Internal Facing

CVE-2009-2761
Unquoted Windows search path vulnerability in the scheduler (sched.exe) in Avira AntiVir, AntiVir Premium, Premium Security Suite, and AntiVir Professional might allow local users to gain privileges via a malicious antivir.exe file in the "C:\Program Files\avira\" directory.

CVE-2012-4350
Multiple unquoted Windows search path vulnerabilities in the (1) Manager and (2) Agent components in Symantec Enterprise Security Manager (ESM) before 11.0 allow local users to gain privileges via unspecified vectors.

CVE-2013-0513
IBM Security AppScan Enterprise 5.6 and 8.x before 8.7 and IBM Rational Policy Tester 5.6 and 8.x before 8.5.0.4 create a service that lacks " (double quote) characters in the service path, which allows local users to gain privileges via a Trojan horse program, related to an "Unquoted Service Path Enumeration" vulnerability.

CVE-2013-1092
Multiple unquoted Windows search path vulnerabilities in Novell ZENworks Desktop Management (ZDM) 7 through 7.1 might allow local users to gain privileges via a Trojan horse "program" file in the C: folder, related to an attempted launch of (1) ZenRem32.exe or (2) wm.exe.

CVE-2013-1609
Multiple unquoted Windows search path vulnerabilities in the (1) File Collector and (2) File PlaceHolder services in Symantec Enterprise Vault (EV) for File System Archiving before 9.0.4 and 10.x before 10.0.1 allow local users to gain privileges via a Trojan horse program.

CVE-2013-1610
Unquoted Windows search path vulnerability in RDDService in Symantec PGP Desktop 10.0.x through 10.2.x and Symantec Encryption Desktop 10.3.0 before MP3 allows local users to gain privileges via a Trojan horse application in the %SYSTEMDRIVE% top-level directory.

MR VULNERABILITY

Vulnerability is the arch enemy of security, resilience and edgescan!

Top CWE Common Weakness Enumeration 2020

Common Weakness Enumeration (CWE™) Software Weaknesses

These weaknesses are dangerous because they are often easy to find or exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working.

The 10 most common CWE discovered in 2020 amounts to **81%** of all CWE discovered in 2020.

For more on CWE see https://cwe.mitre.org/index.html

The 10 most common CWE in 2020

CWE	% of occurrence	Description
CWE-326	19%	Inadequate Encryption Strength
CWE-310	17%	Cryptographic Issues
CWE-200	14%	Exposure of Sensitive Information
CWE-327	12%	Use of a Broken or Risky Cryptographic Algorithm
CWE-20	4%	Improper Input Validation
CWE-119	4%	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-79	3%	Improper Neutralization of Input During Web Page Generation
CWE-416	2%	Use After Free
CWE-787	2%	Out-of-bounds Write
CWE-264	2%	Permissions, Privileges, and Access Controls

> *"...regarding malware and ransomware, something that is overlooked regularly by awareness training is that robust vulnerability & patch management dramatically increases resilience to such attacks...many variants use CVEs which are up to five years old..."*

Malware, Ransomware and CVE's

Throughout 2020, many CVE's were discovered which are used by threat actors to exploit malware, ransomware and cause business disruption. It is important to consider the fact that many of these vulnerabilities were located on non internet facing systems. There is a cultural trend not to focus on internal vulnerabilities, which may result in a ransomware/data exfiltration due to a phishing email or a social engineering attack. Vulnerability management is a core component in the prevention of such risks. It is also worth noting that many of the more common CVE's related to such attacks are between 1 and 3 years old and there are mitigations/patches available.

Frequency and Severity

CVE	Relative Occurrence %	CVSS Score
CVE-2019-0708	28.90%	**9.8**
CVE-2017-0143	26.50%	**8.1**
CVE-2017-5638	13.20%	**10**
CVE-2017-5715	9.10%	**5.6**
CVE-2017-10271	6.30%	**7.5**
CVE-2018-0802	4.20%	**7.8**
CVE-2019-2725	3.50%	**9.8**
CVE-2017-11882	3.10%	**7.8**
CVE-2018-12130	1.40%	**5.6**
CVE-2018-7600	1.00%	**9.8**
CVE-2018-4878	0.70%	**9.8**
CVE-2017-0199	0.70%	**7.8**
CVE-2018-8174	0.70%	**7.5**
CVE-2012-0158	0.70%	**9.3**

Critical risk

High risk

Medium risk

Malware, Ransomware and CVE's

CVE-2019-0708
Malware Name: Bluekeep
Threat Actor: Kelvin SecTeam (Venezuela, Colombia, Peru)

CVE-2017-0143
Malware Name: EternalSynergy and EternalBlue Exploit Kit
Threat Actor: APT3 (China), Calypso (China)

CVE-2017-5638
Malware Name: JexBoss
Threat Actor: Lazarus Group (North Korea)

CVE-2017-5715
Malware Name: Meltdown / Spectre
Threat Actor: Unknown

CVE-2017-10271
Malware Name: Cryptominer
Threat Actor: Rocke Gang (Chinese Cybercrime)

CVE-2018-0802
Malware Name: EXPLOIT.MSOFFICE.CVE-2018-0802
Threat Actor: Cobalt Group (Spain, Ukraine), APT37 (North Korea), Silent Group (Russia), Cloud Atlas (Unknown), Cobalt Group (Spain, Ukraine), Goblin Panda (China), APT23 (China), APT27 (China), Rancor Group (China), Temp.Trident (China)

CVE-2019-2725
Malware Name: Monero
Threat Actor: Panda (China)

CVE-2017-11882
Malware Name: Loki Infostealer
Threat Actor: APT32 (Vietnam), APT34 (Iran), APT40 (China), APT-C-35 (India), Cobalt Group (Spain, Ukraine), Silent Group (Russia), Lotus Blossom (China), Cloud Atlas (Unknown), FIN7 (Russia)

CVE-2018-12130
Malware Name: Metldown2
Threat Actor: Iron Tiger (China), APT3 (China), Calypso (China)

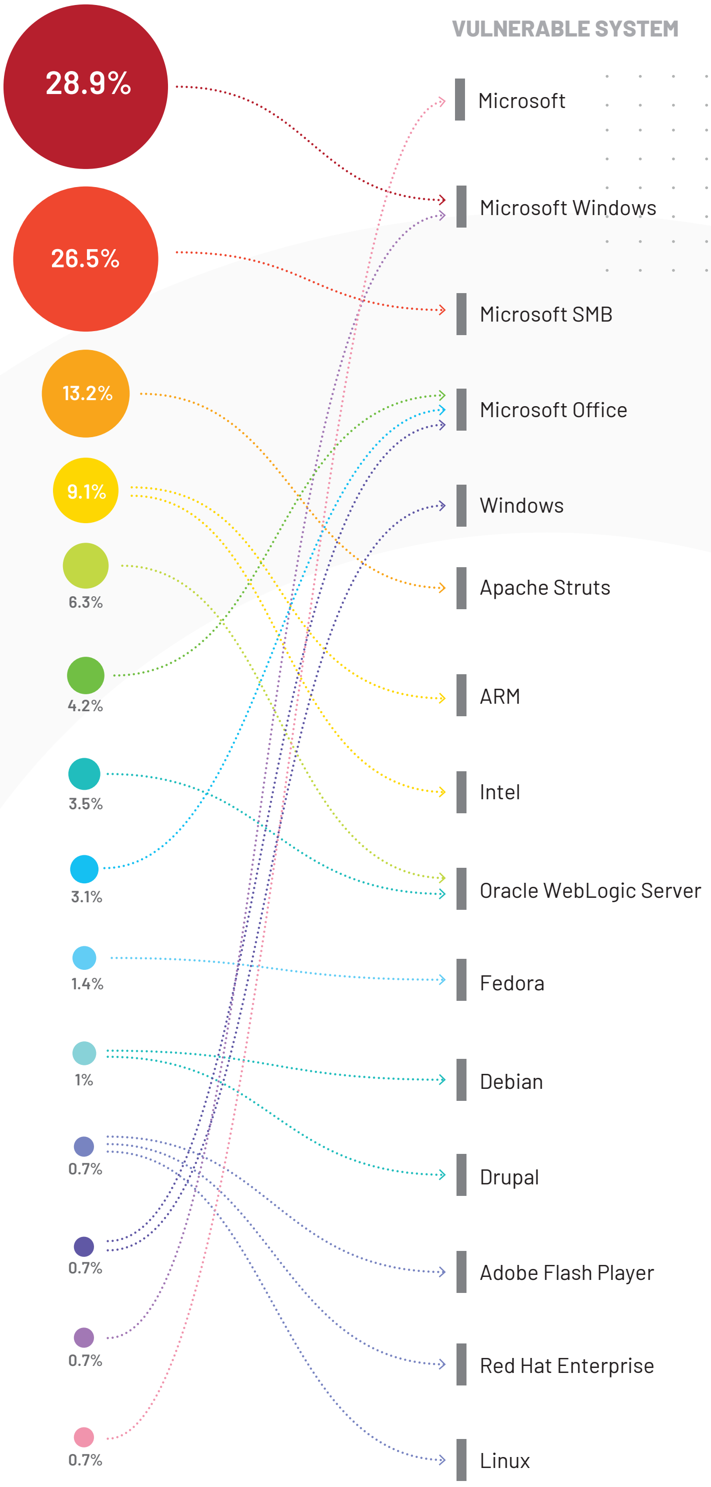
CVE-2018-7600
Malware Name: #drupalgeddon2
Threat Actor: Kelvin SecTeam (Venezuela, Colombia, Peru), Sea Turtle (Iran)

CVE-2018-4878
Malware Name: SWF_EXPLOYT.BL
Threat Actor: APT37 (North Korea), Lazarus Group (North Korea)

CVE-2017-0199
Malware Name: FINSPY
Threat Actor: APT34 (Iran), APT40 (China), APT-C-35 (India), Cobalt Group (Spain, Ukraine), APT37 (North Korea), Silent Group (Russia), Gorgon Group (Pakistan), Gaza Cybergang (Iran)

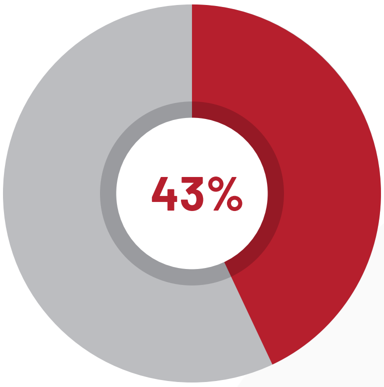
CVE-2018-8174
Malware Name: Monero Miner
Threat Actor: Silent Group (Russia), Dark Hotel APT (North Korea)

CVE-2012-0158
Malware Name: Safe
Threat Actor: APT28 (Russia), APT-C-35 (India), Cobalt Group (Spain, Ukraine), Lotus Blossom (China), Cloud Atlas (Unknown), Goblin Panda (China), Gorgon Group (Pakistan), APT40 (China)

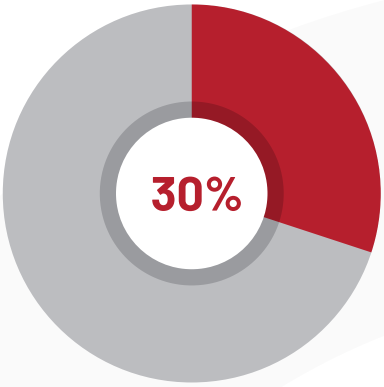


CVE Dispersion and Clustering

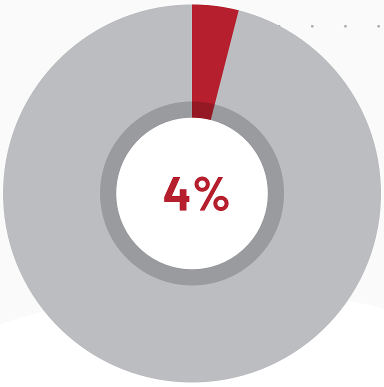
System with at least one CVE



System with more than one CVE



System with more than ten CVEs



This provides a snapshot view of the health of assets in general, both public internet facing and facing hosts combined. **The % of Assets with more than ten CVE's has dropped significantly from 2019** (down from 15.05%) due to a combination of older systems being decommissioned and systems being maintained due to improved visibility via continuous asset profiling.

Organisations have pivoted to a remote working model. The risk profile is changing and they need the data provided in the stats report to understand this.

Exposed – Services and Ports

Edgescans Continuous asset profiling detects exposed ports and services on the public Internet. Unfortunately organisations can have systems exposed which gives rise to an increased attack surface and the potential for a security breach.

Remote desktop (RDP) and Secure Shell (SSH) exposure increased by around 40%, likely due to the increase in remote working due to covid-19. RDP (and similar services) are easy and commonly used avenues for brute force or credential stuffing attacks, against weak user credentials.

Many exposed ports have been used for attacks such as WannaCry, BlueKeep and the Eternal Blue family, but to name a few.

Such exposed ports and services can be victim to traditional hacking attacks which also give rise to breach and data loss.

> *"Remote desktop (RDP) and Secure Shell (SSH) exposures increased by 40%, likely due to the increase in remote working due to Covid-19."*

- Of the sample 1 million public facing Internet endpoints mapped in 2020.
- 21,070 appeared to have an exposed database systems.
- 11,785 systems had exposed Remote Desktop (RDP) services exposed, and increase of 40% on 2019.
- 18,350 of systems had an exposed administration console or API interface (over HTTP/HTTPS).

Sample of one million Endpoints

Protocol/Port	Purpose	Port Number	Protocol	Percentage of exposed services
SSH	Remote system login & management	22	TCP	3.80%
SMTP	Email server / protocol	25	TCP	1.56%
RDP	Remote system login & management	3389	TCP	1.18%
DNS	Domain Name System	53	TCP	0.99%
SNMP	Network & device management	161	UDP	0.89%
FTP	Unencrypted file & data transfer	21	TCP	0.75%
RPC	Client-Server communication	135	TCP	0.66%
NetBios	Internal (LAN) communication	139	TCP	0.57%
POP3	Internal (LAN) communication	110	TCP	0.50%
SQL Server	Enterprise database engine	1443	TCP	0.49%
MySQL DB	Enterprise database engine	3306	TCP	0.48%
Oracle DB	Enterprise database engine	1521	TCP	0.47%

Edgescan Heroes and Villains

The Edgescan Heroes and Villains are a series of characters representing cyber security and infosec challenges and the tactics we use to fight against these threats. The 'bad guys' are Mr Vulnerability, False Positive, Budget Burn, Snake Oil and Miss Information. Their attacks are defended by the 'good guys', Mapper, Infinity, Scale and Validator. While the heroes all have their super powers, their main strength is that they are powered by Edgescan.

MAPPER

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

INFINITY

Assessment on an infinite scale. Never gets tired.

SCALE

Nothing is too big for scale. Scale supports accuracy and coverage.

VALIDATOR

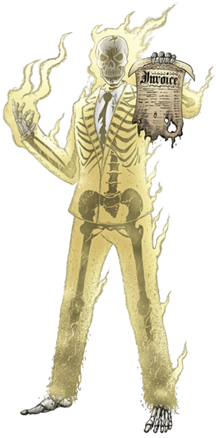
She never makes mistakes. Identifies real risks and helps the team focus on what matters.

MR VULNERABILITY

Vulnerability is the arch enemy of security, resilience and Edgescan!

FALSE POSITIVE

Master of deception, loves sapping resources and burning time.



BUDGET BURN

Loves to burn resources and time on tasks. Snake oil is his best friend.

MISS INFORMATION

Miss Information, spreads fear, fake news and cyber ignorance.

SNAKE OIL

A joker and scoundrel. Never a true word can be said by snake oil. Loves building up your hopes only to let you down with a bang!!

What is Edgescan?

Application Security

- Continuous Application/API vulnerability assessment
- Pentesting as a Service (PTaaS)
- API Security assessment and Pentesting

Host Security

- Continuous External / Internal Vulnerability Assessment
- Pentesting as a Service (PTaaS)
- Daily updated Know Vulnerabilities (CVE) database

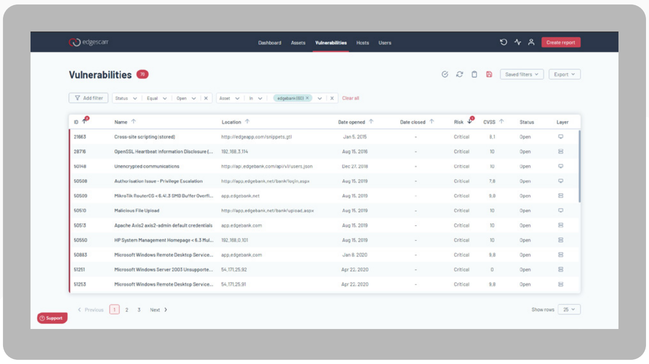
Continuous Monitoring

- Live system and service 24/7 discovery
- Exposed service alerting
- 24 x 7 x 365 Asset Visibility

API Discovery

- Continuous API discovery and enumeration.
- Eliminate blind spots
- Multi-layer probing technology

- Fullstack coverage
- Validated by experts
- Mitigation Support
- On-demand
- Alerting and integration



ID	Name	Location	Date opened	Date closed	Risk	CVSS	Status	Layer
21663	Cross-site scripting (stored)	http://edgeapp.com/snippets.gtl	Jan 5, 2015	-	Critical	8.1	Open	🖥
28716	OpenSSL Heartbeat Information Disclosure (...	192.168.3.114	Aug 15, 2016	-	Critical	10	Open	🗄
50148	Unencrypted communications	http://api.edgebank.com/api/v1/users.json	Dec 27, 2018	-	Critical	10	Open	🖥
50508	Authorisation Issue - Privilege Escalation	http://app.edgebank.net/bank/login.aspx	Aug 15, 2019	-	Critical	7.8	Open	🖥
50509	MikroTik RouterOS < 6.41.3 SMB Buffer Overfl...	app.edgebank.net	Aug 15, 2019	-	Critical	9.8	Open	🗄
50510	Malicious File Upload	http://app.edgebank.net/bank/upload.aspx	Aug 15, 2019	-	Critical	10	Open	🖥
50513	Apache Axis2 axis2-admin default credentials	app.edgebank.com	Aug 15, 2019	-	Critical	10	Open	🗄
50550	HP System Management Homepage < 6.3 Mul...	192.168.0.101	Aug 15, 2019	-	Critical	10	Open	🗄
50883	Microsoft Windows Remote Desktop Service...	app.edgebank.com	Jan 8, 2020	-	Critical	9.8	Open	🗄
51251	Microsoft Windows Server 2003 Unsupporte...	54.171.25.92	Apr 22, 2020	-	Critical	0	Open	🗄
51253	Microsoft Windows Remote Desktop Service...	54.171.25.91	Apr 22, 2020	-	Critical	9.8	Open	🗄

What does Edgescan do?

Simply, we detect & validate cyber vulnerabilities in your IT systems; Web, Network, API, CI/CD, IoT, Internal, external – fullstack!

We provide continuous visibility to help you maintain security. We provide on-demand Pen Testing as a Service (PTaaS).

Why should I use Edgescan?

We deliver a dedicated vulnerability detection solution (SaaS). We're extremely accurate and provide support to guide you through your journey.

We deliver a comprehensive and cost effective solution. We're PCI Approved Scanning Vendors.

40%

Reduce Mean Time To Remediation (MTTR) by 40%

2.1+

Save on average the equivalent of 2.1 full time staff members per month using Edgescan

edgescan™

What is Edgescan?

What's different?

- All vulnerabilities are validated for accuracy and risk.
- We're a fullstack cyber SaaS (Web applications and Network security).
- We support our clients to help understand and fix with our certified penetration testing team.
- We can scale to thousands of assessments.
- Fixed monthly fee, unlimited assessments.

What are the main features?

- Continuous fullstack security testing.
- Automatic assessments of new endpoints as they are discovered.
- Validation and support for all issues discovered.
- Continuous asset and API monitoring and detection.
- Internal and External Assessments
- On-demand assessments and penetration testing.
- Alerting and Integration customizable for you.

Does this help me?

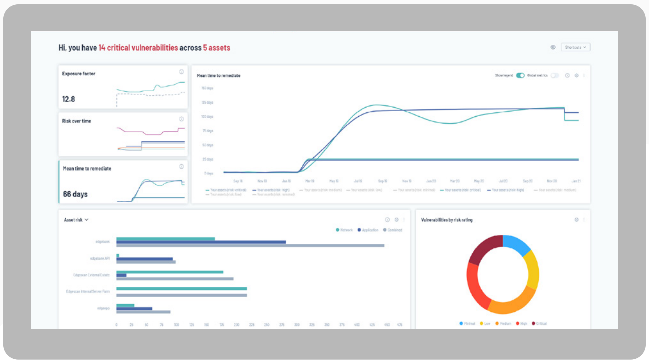
The Edgescan Team are experts at vulnerability detection. We save you time and money by helping you focus on items that matter.

How?

We deliver a cyber assessment service from our cloud which provides continuous and on-demand detection.

Why?

Finding weaknesses in IT Systems helps prevent a data breach or cyber attack.



Hi, you have 14 critical vulnerabilities across 5 assets

If you think Edgescan can help your organisation increase its security posture, get in touch with our sales team for a trial at sales@edgescan.com.

100%
Full OWASP Application Security Coverage

24/7/365
Continuous asset profiling and discovery

Gartner.

SC Awards 2020 EUROPE WINNER Best Vulnerability Management Solution

aws partner network

PCI Security Standards Council APPROVED SCANNING VENDOR™

Contributor Verizon 2019 Data Breach Investigations Report

ISO 27001 CERTIFICATION EUROPE™

2019 Tech Excellence Awards Managed Security Service Provider of the Year Edgescan

CREST

2020 Computing Security Awards WINNER Penetration Testing Solution of the Year

The Irish Advantage

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 Exposure

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 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

IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

Sales and general enquiries:
sales@edgescan.com

@edgescan
in @edgescan

edgescan.com