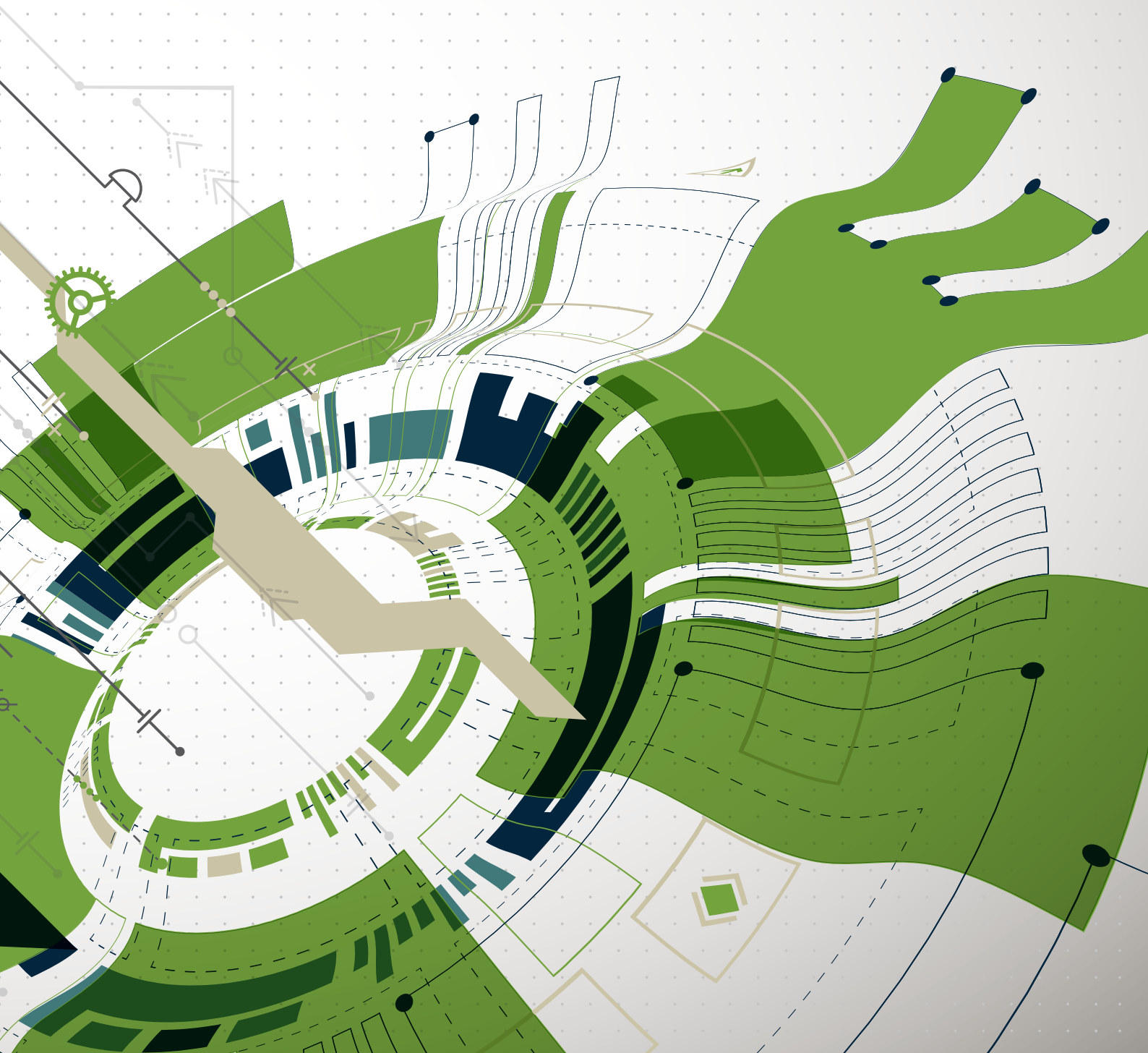
edgescan™

FULLSTACK VULNERABILITY MANAGEMENT™

2020 VULNERABILITY STATISTICS REPORT



WELCOME

For our 5th Year, welcome to the Edgescan Vulnerability Stats Report. This report aims to demonstrate the state of full stack security based on thousands of full stack assessments globally, delivered by the Edgescan SaaS during 2019. This report is still a joy to do as it gives decent insight into what's going on from a trends and statistics perspective and overall state of cyber security. Sometimes a curveball or outlier statistical result leaves you scratching your head, but that's the nature of statistics!

The Edgescan report has become a reliable source for truly representing the global state of cyber security. This year we took a deeper look at vulnerability metrics from a known vulnerability (CVE) and visibility standpoint (exposed services), coupling both non-public (i.e internal) and public Internet-facing systems.

We still see high rates of known (i.e. patchable) vulnerabilities which have working exploits in the wild, possibly demonstrating that it is hard to patch production systems. The MTTR (Mean Time to Remediation) stats also reflect on this issue. Effective patching on a consistent basis still appears to be a challenge, but also detection on a constant basis needs improvement.

Web application security 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.

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. The assumption here is that enterprises simply did not have the visibility or systems in place, to make them aware or inform them of the exposure.

As per the 2019 report, we also delve into "internal" cyber security, looking at metrics which may not seem as important, but are a valuable defence in the case of APT, malware infection, ransomware or other internal attacks. These 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 how to prioritize on what is important, as not all vulnerabilities are equal.

Best regards,

EOIN KEARY

Founder,
Edgescan.com

edgescan

2019 – A REVIEW

VULNERABILITY VALIDATION IS STILL A PROBLEM

More than 60% of security professionals estimate that their organisations security function, spend over 3 hours per day validating false-positives, according to our 2019 cyber survey at Infosecurity Europe.*

HOT IN THE CITY

Malware "hit the city" in 2019, which was leveraged to compromise entire local governments and councils. Dozens of cities were hit by coordinated ransomware attacks that forced services offline and demanded payment for restoration. Some cities even capitulated and paid the ransoms.

PHISHING

Phishing gained popularity, more so via Business Email Compromise (BEC) techniques. Some threat agents were noted as being highly sophisticated in their approach.

ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) and Machine Learning (ML) have been high on the investment radar for some time, however it appears in early 2020 that the paradigm is losing some of its shine. The market is realising plenty of snake oil relating to AI technologies, but we will have to wait and see if the dial moves in a positive direction this year, as a result of significant AI marketing and investment in 2019.

2019 - CYBER SKILLS SHORTAGE

Not surprisingly, the current cyber security skills shortage is being experienced by the security professionals who responded to the survey. Only 32% feel they are fully-staffed and the remainder, 68%, need more staff to manage their organisation's cyber security and comfortably deal with vulnerability intelligence.

CONFIDENCE IS KING

Despite AI/ML and investment in cyber, only a small percentage of organisations believe they have a high degree of confidence in their ability to measure, mitigate and manage cyberattacks.

ASSET MANAGEMENT

Worryingly, 64% of professionals admitted to not being fully aware of their organisation's web applications or end-points. Many security professionals are not alarmed by this lack of awareness, as nearly 68% believe their visibility is 'average' while acknowledging they do not monitor some connected devices. This amounts to a significant gap in asset visibility for most organisations.

BREACHES

More than 8 Billion records were breached in 2019. A few examples: Quest Diagnostics: 11.9 mil, Houzz: 48.9 mil, Capital One: 100 mil, Dubsmash: 161.5 mil, Zynga: 218 mil – Many of which were web application layer vulnerabilities and were preventable issues, if appropriate secure development and visibility practices were adhered to.

* https://www.edgescan.com/infosecurity-europe-2019-survey-results

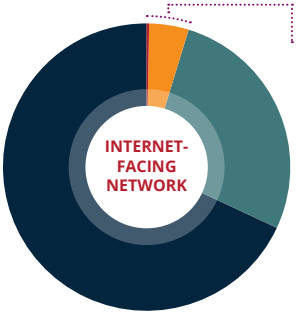
RISK DENSITY

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).

INTERNET-FACING NETWORK

0.51% CRITICAL
4.28% HIGH
27.38% MEDIUM
67.83% LOW

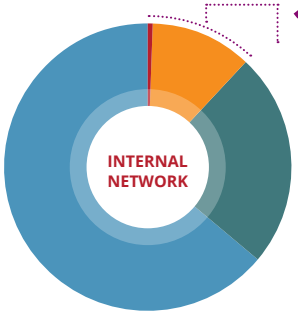


4.79% OF ALL VULNERABILITIES WERE HIGH OR CRITICAL RISK

27.38% OF ALL VULNERABILITIES WERE MEDIUM RISK

INTERNAL NETWORK

0.57% CRITICAL
11.6% HIGH
24.11% MEDIUM
63.72% LOW

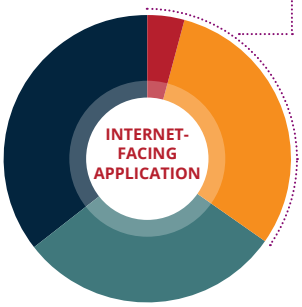


12.17% OF ALL VULNERABILITIES WERE HIGH OR CRITICAL RISK

24.11% OF ALL VULNERABILITIES WERE MEDIUM RISK

INTERNET-FACING APPLICATION

4.4% CRITICAL
30.38% HIGH
29.8% MEDIUM
35.42% LOW

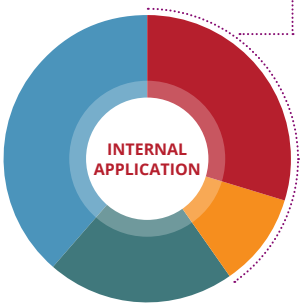


34.78% OF ALL VULNERABILITIES WERE HIGH OR CRITICAL RISK

29.8% OF ALL VULNERABILITIES WERE MEDIUM RISK

INTERNAL APPLICATION

29.82% CRITICAL
10.53% HIGH
21.05% MEDIUM
38.6% LOW



40.35% OF ALL VULNERABILITIES WERE HIGH OR CRITICAL RISK

21.05% OF ALL VULNERABILITIES WERE MEDIUM RISK

Externally facing web applications still have a significantly higher Risk Density, with 34.78% of vulnerabilities discovered rated as High or Critical Risk, compared to externally facing network layer systems, with a High or Critical risk density of just 4.79%.

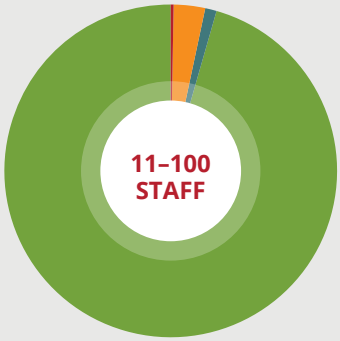
RISK DENSITY BY ORGANISATION SIZE

PERCENTAGE OF ALL VULNERABILITIES DISCOVERED IN 2019

We analysed risk density when applied to the size of an organisation, from SME's to large enterprises. For small organisations (with 11-100 staff) we can see the combined Medium + High + Critical Risk % of all vulnerabilities is **4.1%.** This is likely due to such organisations simply having a smaller digital estate and thus attack surface.

For larger organisations, the risk density is largely similar, i.e. for organisations with 100+ staff, a similar risk density profile can be found.

0.1% CRITICAL
3% HIGH
1% MEDIUM
95.9% LOW



1% CRITICAL
13% HIGH
21% MEDIUM
65% LOW

0.5% CRITICAL
11% HIGH
29% MEDIUM
59.5% LOW

1% CRITICAL
10% HIGH
19% MEDIUM
70% LOW

14% of vulnerabilities for organisations with a staff size of 101-1000 are high or critical risk.

11.5% of vulnerabilities for organisations with a staff size of 1001-10000 are high or critical risk.

11% of vulnerabilities for organisations with a staff size of 10001+ are high or critical risk.

MTTR

MEAN TIME TO REMEDIATE (MTTR) VULNERABILITIES. TOTAL AVERAGE ACROSS BOTH WEB APPLICATIONS AND INFRASTRUCTURE VULNERABILITIES (FULL STACK):

MTTR for internet-facing vulnerabilities: 84.59 days

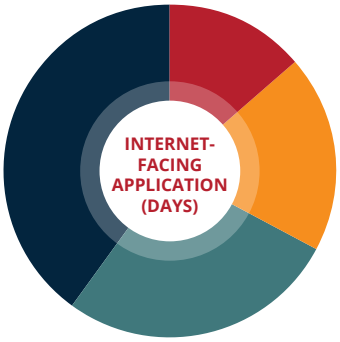
MTTR for non-public/ internal vulnerabilities: 75.29 days

INTERNET-FACING APPLICATION

50.55 DAYS
CRITICAL VULN

69.7 DAYS
HIGH VULN

98.92 DAYS
MEDIUM VULN

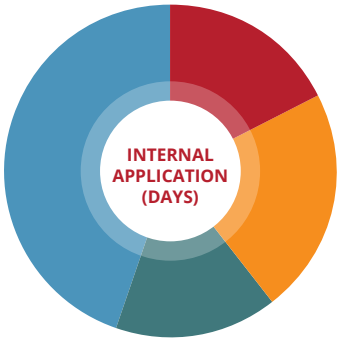


INTERNAL APPLICATION

64 DAYS
CRITICAL VULN

81 DAYS
HIGH VULN

57 DAYS
MEDIUM VULN

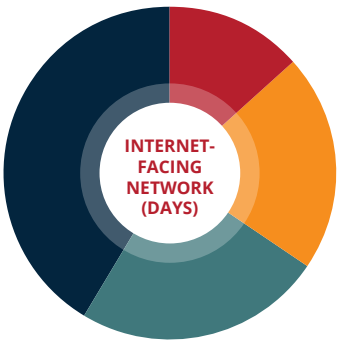


INTERNET-FACING NETWORK

49.26 DAYS
CRITICAL VULN

77.12 DAYS
HIGH VULN

88.73 DAYS
MEDIUM VULN

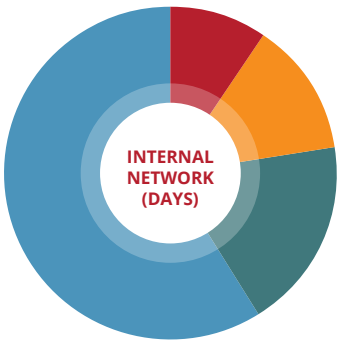


INTERNAL NETWORK

34.76 DAYS
CRITICAL VULN

48 DAYS
HIGH VULN

67.8 DAYS
MEDIUM VULN



A curious item to be noted here is the MTTR for critical risk internal network layer vulnerabilities – the MTTR was **34.76 days** which is significantly faster than the MTTR for internet-facing network layer critical vulnerabilities, which stands at **49.26 days**. This is likely due to the slower speed and overhead at which "live" production environments can be patched. A strong cloud deployment process using immutable images (i.e. issuing a refreshed build) would generally help improve MTTR, as "Patching" in the traditional sense is not required.

The MTTR for critical risk public Internet facing **web application vulnerabilities** and critical risk public Internet facing **network vulnerabilities** is similar at **50.55 days** and **49.26 days** respectively.

MTTR BASED ON COMPANY SIZE

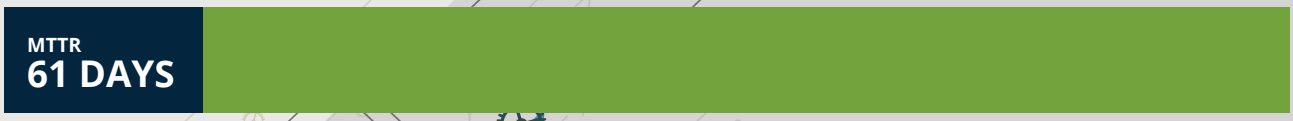
We measured time-to-fix for critical risk vulnerabilities, based on organisation size. While small organisations seem to fare the worst, likely due to lack of expertise or resources, it appears that company size generally has little or no impact in relation to the time spent to close a critical vulnerability.

STAFF COUNT: 11-100

STAFF COUNT: 101-1000

STAFF COUNT: 1001–10000

STAFF COUNT: 10000+



CVE LANDSCAPE

Oldest vulnerability discovered in 2019: 20 years old (1999)

Occurrence Rate of 20-year-old vulnerability: 1.75%

Most Common Vulnerability from 1999: CVE-1999-0517

An SNMP community name is the default (e.g. public, null, or missing)

Base CVSS Score (2.0): 7.5 (High)

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

Most Common (CVE) Vulnerability discovered in 2019: CVE-2016-2183

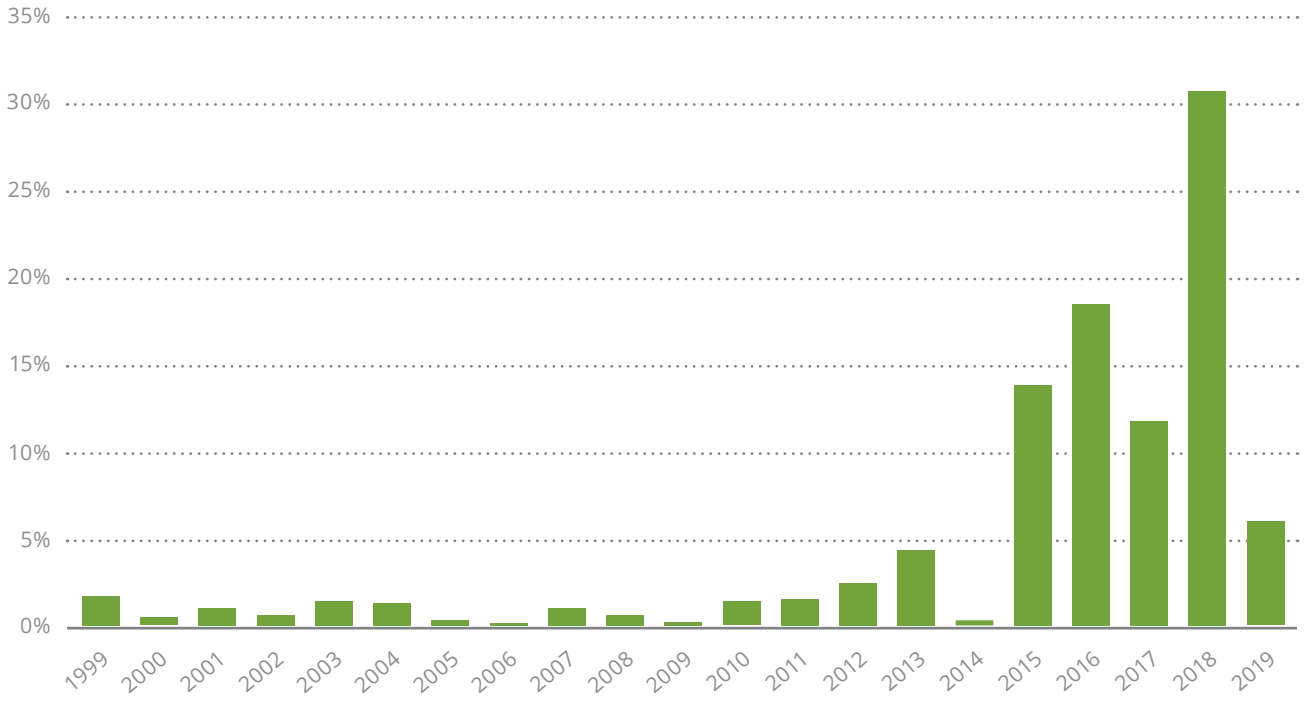
The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session,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

Base CVSS (3.0) Score: 7.5 (High)

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

*As per NIST National Vulnerability Database (NVD) https://nvd.nist.gov/

% OF ALL DISCOVERED CVE’S



CVE PATCHING SPEED – PATCHING KNOWN VULNERABILITIES

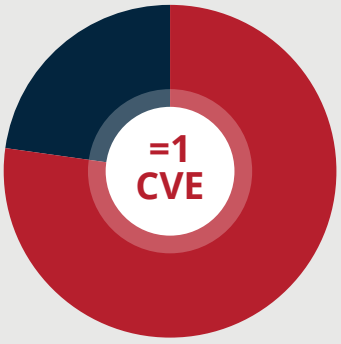
Average time to patch an internal system is **50 days**, but **71 days** for an Internet-facing system.

On average **67.8%** of assets had at least one CVE with a CVSS score of 4.0 or more. From a PCI DSS standpoint, this would result in an average of **67.8%** of assets failing PCI compliance!

On average **27%** of assets had a CVE with a CVSS score of 7.0 or more.

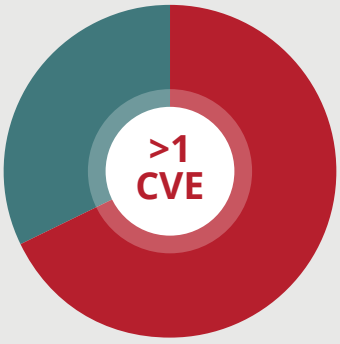
CVE DISPERSION AND CLUSTERING

77.36%



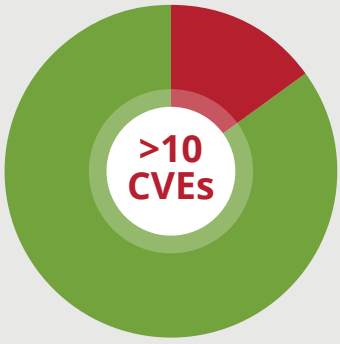
SYSTEMS WITH AT LEAST ONE CVE

67.67%



SYSTEMS WITH MORE THAN ONE CVE

15.05%



SYSTEMS WITH MORE THAN TEN CVEs

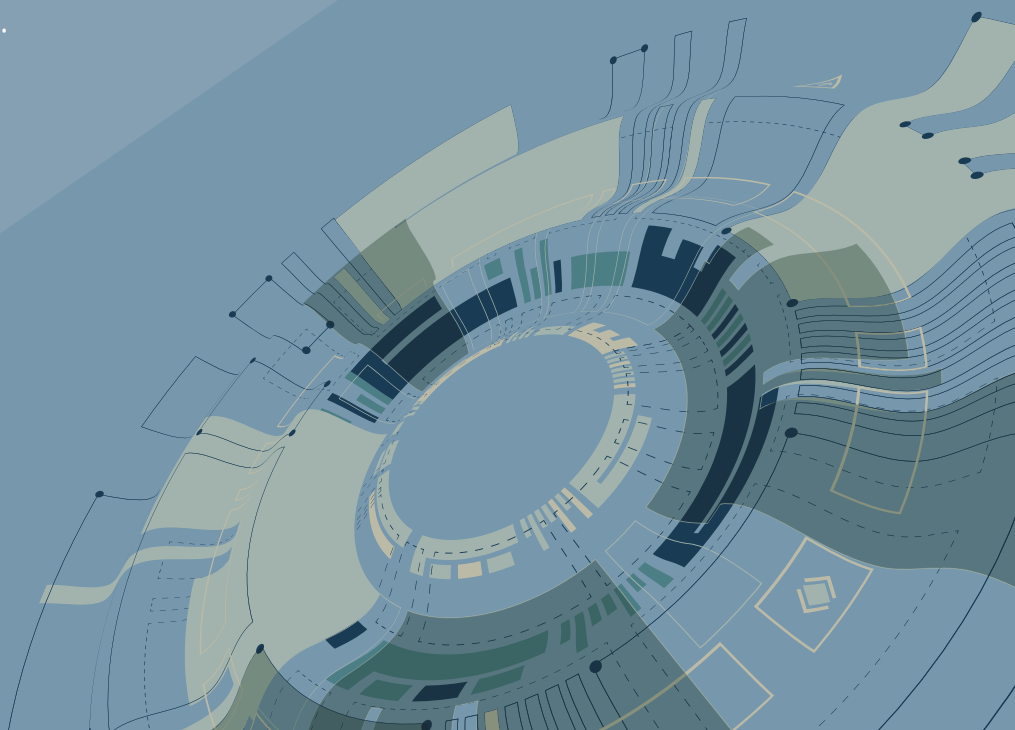
VULNERABILITY TAXONOMY

Earlier in the report, we discuss the rates of vulnerabilities across both Web Applications and Hosting environments, what we refer to as a 'full stack view'. Another aspect which is also interesting, and covered in the next section, is to delve into the type of vulnerabilities being discovered. These tease out some of the root causes, be it technical, logical, patching-related or a coding issue.

The following is a high-level breakdown of the most common critical vulnerabilities discovered and validated in 2019, by the Edgescan SaaS.

Obviously there are thousands of different vulnerabilities discovered in a 12 month period and below focuses on some of the more interesting or common ones.

With access to all of this fascinating information, we thought, why not single-out the most common critical risks across the full stack and maybe, if folks focus on preventing these particular issues, then things might improve a little...



MOST COMMON CRITICAL RISK VULNERABILITIES IN 2019 (INTERNAL / NON PUBLIC FACING)

18%
BLUEKEEP CVE-2019-0708

This is a security vulnerability that was discovered in Microsoft's Remote Desktop Protocol implementation, which allows for the possibility of remote code execution.

17%
UNSUPPORTED SQL SERVER

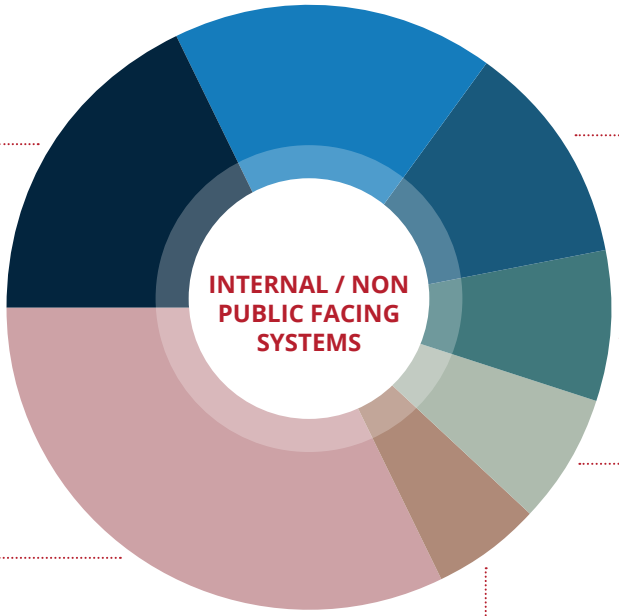
A version of Microsoft SQL Server is running on the host which is no longer supported by the vendors. The results in no additional patching or fixes being issued for any subsequently discovered vulnerabilities. This system is considered end-of-life and should be replaced.

12%
SQL INJECTION (WEB APPLICATION ATTACK)

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.



8%
MS OFFICE CVE-2017-11882

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability."

This vulnerability was commonly used in 2019 by malware varients such as Emotet, a malicious modular banking trojan.

32%
OTHER

6%
SMB MS17-010/ CVE-2017-0143 TO CVE-2017-0148

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, SMB Remote Code Execution Vulnerability.

7%
RDP MS12-020/ CVE-2012-0002

The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code.

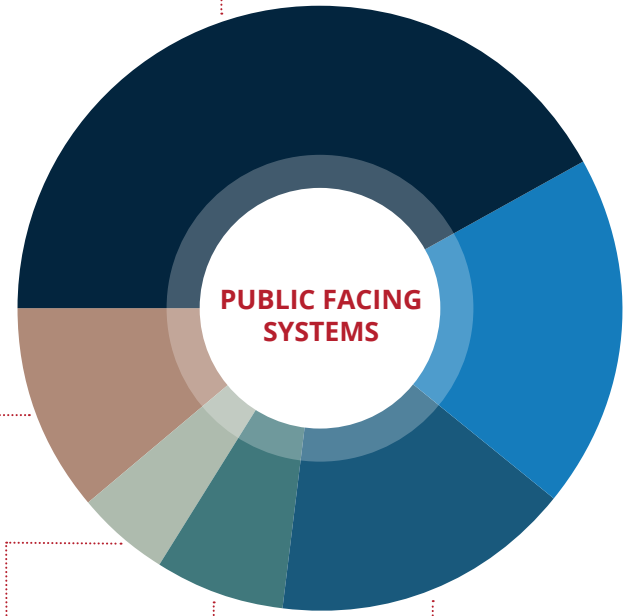
MOST COMMON CRITICAL VULNERABILITIES IN 2019 (INTERNET FACING)

42%
SQL INJECTION

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.



19%
CROSS-SITE SCRIPTING (XSS)

Cross site Scripting (XSS) attacks are a type of injection problem, in which malicious scripts are injected into web sites. Cross site scripting flaws are the most prevalent flaw in web applications today. Cross site scripting attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser-side script, to a different end user.

The 'stored' variant is considered a "Critical" vulnerability as it persists across all users who access an infected page and has the potential to infect a wide user base of the web application or site.

11%
OTHER

5%
SENSITIVE FILE DISCLOSURE

This is the result of leaving unprotected files on a hosting environment, systems using inadequate authorization or poorly deployed systems which result in directory listing and sensitive data disclosure.

A recent trend in such a vulnerability, are exposed AWS S3 buckets which are misconfigured, resulting in publicly exposed database back up files, internal files, configuration files and other private information being left available on the public Internet.

7%
REMOTE CODE EXECUTION

Remote code execution (RCE) is used to describe an attacker's ability to execute arbitrary commands or code remotely across the Internet or network on a target machine.

This is achieved by exploiting a vulnerability which generally, if known about, could be mitigated via a patch or configuration change.

16%
PHP MULTIPLE VULNERABILITIES

Many PHP vulnerabilities were discovered with ratings including both high and critical risk. Many PHP deployments have multiple vulnerabilities concurrently. PHP is still a widely used programming language but loosing popularity. Millions of sites on the Internet use PHP and will for some time to come.

CVE-2016-7411, CVE-2016-7412, CVE-2014-9425, CVE-2014-9709, CVE-2015-1351, CVE-2015-1352, CVE-2015-8383, CVE-2015-8386, CVE-2015-8387, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8393, CVE-2015-8394, CVE-2015-8865, CVE-2016-3141, CVE-2016-3142, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4537, CVE-2016-4539, CVE-2016-4540, CVE-2016-4542, CVE-2016-5385, CVE-2016-5399, CVE-2016-6207, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6293, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297, CVE-2016-7124, CVE-2016-7125, CVE-2016-7126, CVE-2016-7127, CVE-2016-7128, CVE-2016-7129, CVE-2016-7130, CVE-2016-7131, CVE-2016-7132

Critical Risk Vulnerabilities may result in complete compromise of a system or a user. They are generally highly likely to occur, high impact or both.

SQL Injection was first discovered in 1998 and still lives happily on the internet today with its cousins XSS and RCE.

Cross Site Scripting (XSS) was discovered in 1999 and is massively prevalent across web applications today. Easy to discover, harder to develop a weaponised exploit.

MOST COMMON VULNERABILITIES ACROSS THE FULL STACK 2019

39.7%
CRYPTO WEAKNESSES

Implementation of configuration issues relating to TLS/SSL, SSH, PKI encryption. Also including key management and strength configurations. The high levels of crypto weakness detection is not surprising given the billions of endpoints on the web and the historical implementation flaws of SSL which are still not uncommon on the Internet.

12%
CROSS-SITE SCRIPTING (XSS)

Execution of injected client-side code which can be used to deface or steal a users credentials or personal data. XSS attacks can also be used to proliferate malware, redirect users to phishing sites and generally attack legitimate users of your system. This metric includes both persistent, DOM and reflected XSS attack variants.

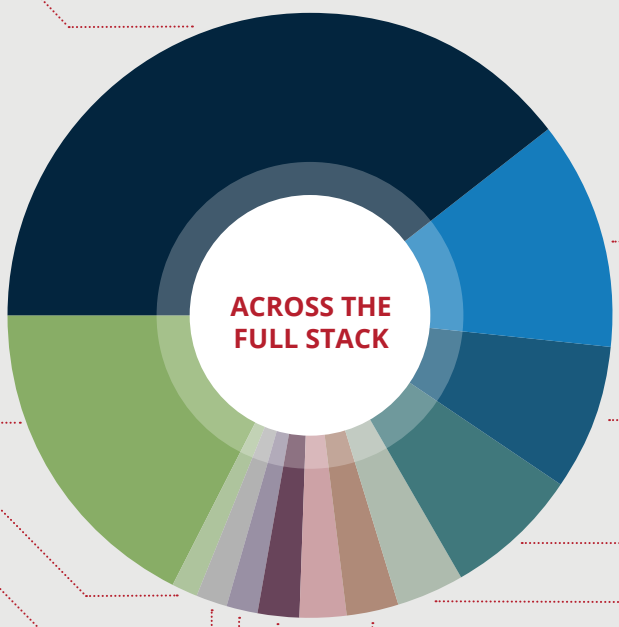
8%
SYSTEM PATCHING RELATED

Systems requiring a security patch due to a known vulnerability (CVE) in existence.

17.4%
OTHER

1.3%
PASSWORD MANAGEMENT AND AUTHENTICATION WEAKNESSES

Unfortunately, weak passwords are still commonplace. Systems accepting weak passwords upon registration, password reset or the lack of multifactor authentication on critical systems, has resulted in large data breaches affecting thousands of users, using a relatively simple attack called “credential stuffing”.



7.1%
DISCLOSURE/ DIRECTORY LISTING

Disclosure of sensitive data, database tables, files or configuration parameters which are a breach of privacy or can be used to gain a further foothold in a system. A recent trend in such a vulnerability are exposed AWS S3 buckets and cloud storage, which are misconfigured, resulting in publicly exposed database back up files, internal files, configuration files and other non-public information being left available on the public Internet.

1.7%
REMOTE CODE EXECUTION

Vulnerabilities relating to the execution of exploit code or malware attacks which may give rise to Ransomware or data theft exploitation.

3.5%
EXPOSED SYSTEMS & SERVICES

FTP, Admin consoles, SSH, RDP, SMB

1.8%
XML EXTERNAL ENTITY ATTACK

An XML External Entity (XXE) attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, server side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts. – OWASP.org

2.2%
INJECTION EXPLOITS

Injection related vulnerabilities such as SQL Injection, LDAP Injection, XML API Injection or Operating System (OS) command injection attacks. Injection attacks as a % of overall vulnerabilities discovered is low, but are still a relatively high occurrence of critical risk issues discovered.

2.4%
AUTHORIZATION & SESSION WEAKNESSES

Weaknesses with session management of web applications or authorization issues relating to access to data or system functionality. Authorization flaws can be difficult to discover using automation alone, given such issues are generally unique per web application.

2.9%
POOR CONFIGURATION

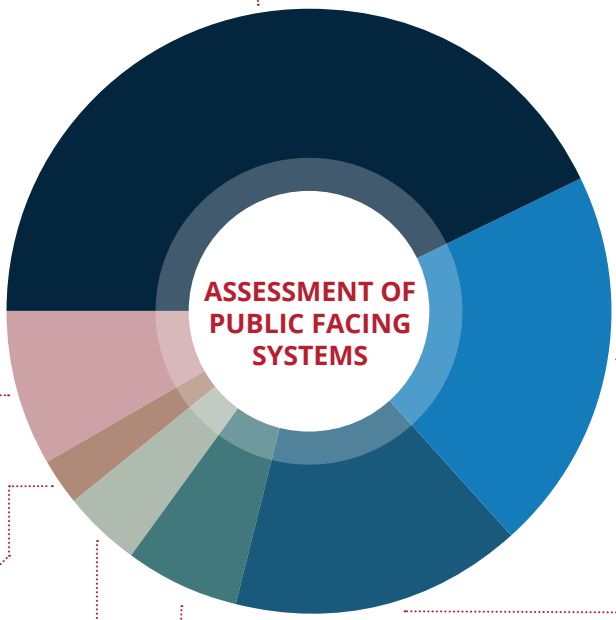
Weak configuration of systems resulting in fail-open situations and access to either data or system functionality not designed to be available. Poor configuration of systems can result in data breach or used as a pivot point to further gain a foothold in a compromised system.

MOST COMMON VULNERABILITIES FOUND VIA UNAUTHENTICATED ASSESSMENT OF PUBLIC INTERNET FACING SYSTEMS

43.05%
CRYPTOGRAPHIC VULNERABILITIES

Vulnerabilities related to the deployment of cryptography between systems and end users, clients and API endpoints.

OpenSSH & OpenSSLVulnerabilities, SSH Weak Algorithms, SSL (SWEET32), SSL DROWN, SSL V2/V3 Protocol Detection, SSL/TLS LogJam, SSL/TLS FREAK, SSL/TLS BEAST, SSL/TLS: Weak Cipher Suites, SSLv3 POODLE, TLS CRIME, Deprecated TLS Versions enabled.



20.3%
WEB APPLICATION RELATED VULNERABILITIES

Types of vulnerabilities relate specifically to development of secure web applications and does not include framework patches, disclosure or crypto issues.

Cross Site Scripting, External Service Interaction (DNS/ HTTP), CORS, CSRF, Cookie Security, Vulnerable JavaScript, SQL Injection, XXE Vulns, Direct object access, Authorization vulnerabilities, Server-side template injection, LDAP Injection, Xpath Injection.

8.08%
OTHER

15.59%
CVE/PATCHING RELATED VULNERABILITIES

Various types of vulnerability where remediation strategy is to apply a patch which is already available.

Examples include: Apache various vulnerabilities, Apple OSX Vulnerabilities, Cisco Various, Citrix Netscalar Vulns, ESXi Vulnerabilities, Flash Security, ISC BIND vulnerabilities, Jboss Vulns, Microsoft IIS Information Disclosure Vulnerabilities, OS End of Life/Deprecated Systems, EternalBlue/Bluekeep, Moodle Security Vulns, Nginx Vulnerabilities, PHP Vulnerabilities, Webmin Vulns, Wordpress, Zend, Spring, Struts, .Net MVC vulnerabilities.

2.48%
INJECTION VULNERABILITIES

Vulnerabilities relating to Buffer overflows, RCE CVE's, Command Injection, but excluding SQL, LDAP, Xpath and XXE, which are already included under Web Application related vulnerabilities.

Injection related vulnerabilities are generally critical risk in nature if they can be validated as being exploitable. The following CVE's are examples of detected injection vulnerabilities throughout 2019.

CVE-2019-3396, CVE-2018-0103, CVE-2018-0104, CVE-2016-1482, CVE-2014-7140, CVE-2018-7600, CVE-2019-0708, CVE-2017-2641, CVE-2018-14631, CVE-2015-1635, CVE-2015-4116, CVE-2016-3132, CVE-2012-2376, CVE-2019-12840, CVE-2015-5080, CVE-2011-0411, CVE-2011-1926,

4.22%
SYSTEM EXPOSURE

Exposure of systems one would generally not like to see on the public Internet. Such systems should not be open to the internet and may also have associated vulnerabilities.

In particular exposed AWS S3 buckets, databases etc., may result in a significant data breach with little or no effort on behalf of the threat actor.

Types of systems here include Databases, Admin Consoles, Software development tools, Security tools, API's, RPC's, etc.

6.28%
INFORMATION DISCLOSURE

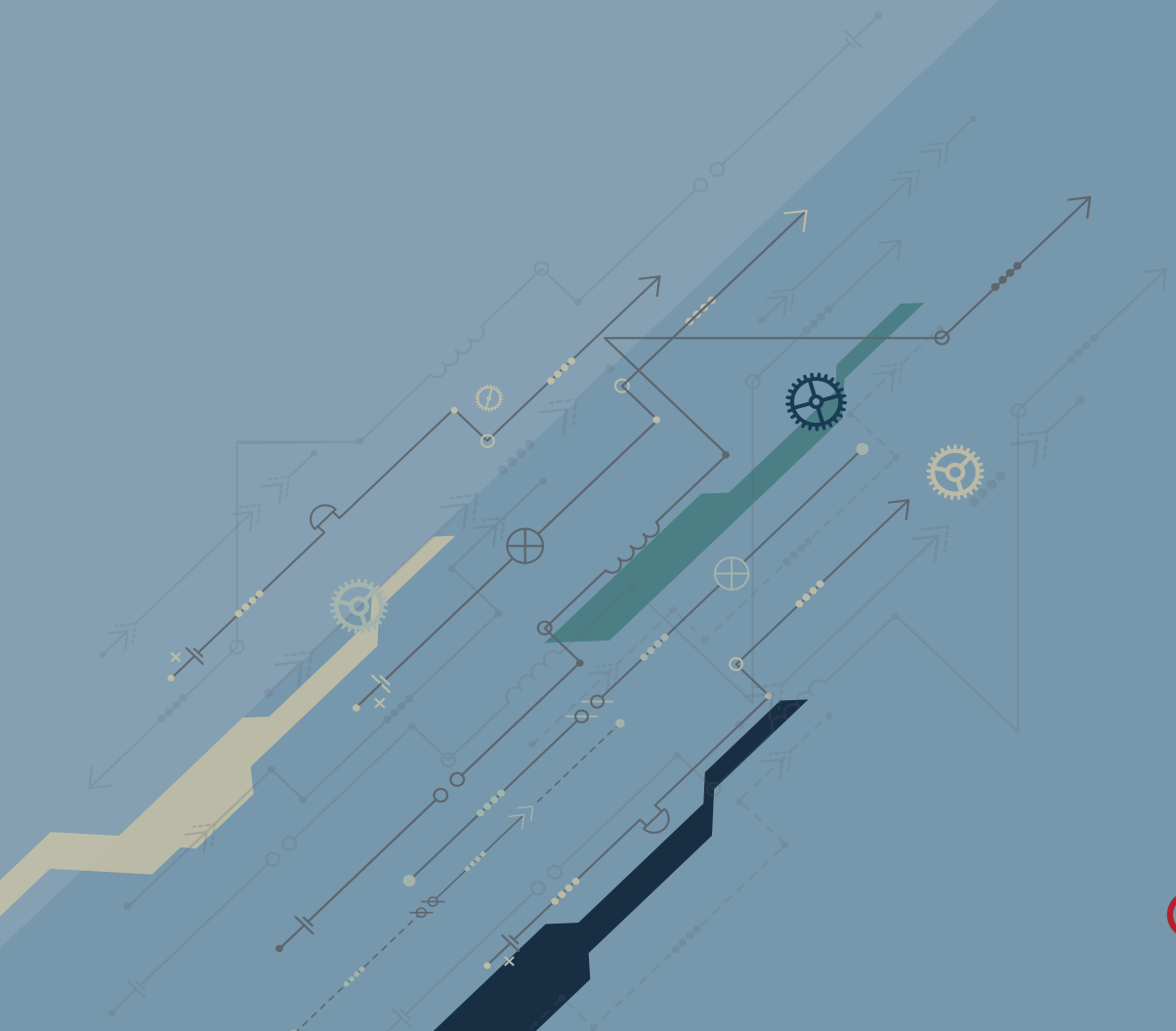
Data and information disclosed in error which may be sensitive in nature, or provide an attacker with additional information in order to pivot into your network, web applications or systems in general. Items such as Directory Listing, Default Index Page, Default Configuration, Sensitive data disclosure, all may result in privacy breach and possibly regulatory (e.g. CCPA, GDPR) penalties!

The high % of cryptographic vulnerabilities is due to flaws in the design, supporting maths and implementation. Generally not a fault of developers or maintenance teams.

Web application vulnerabilities are still commonplace and the leading cause of risk for the past 5 years.

System exposure is generally the result of poor visibility. Exposed services and systems are as easy to find as a haystack in a pile of needles.

Unauthenticated vulnerabilities are exposed without the need for any credentials or privileges. In the case of public facing systems they are simply exposed vulnerabilities ripe for exploitation...



EXPOSED – SERVICES & PORTS

Continuous asset profiling detects exposed ports and services on the public Internet. Unfortunately, organisations unintentionally expose systems which gives rise to an increased attack surface and the potential for a security breach. Systems such as remote desktop, SMB, Database, Telnet etc, are examples of these.

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.

Of the sample 2 million public-facing Internet endpoints mapped in 2019, 3.7% appeared to have an exposed database system

1.93% had insecure FTP services enabled

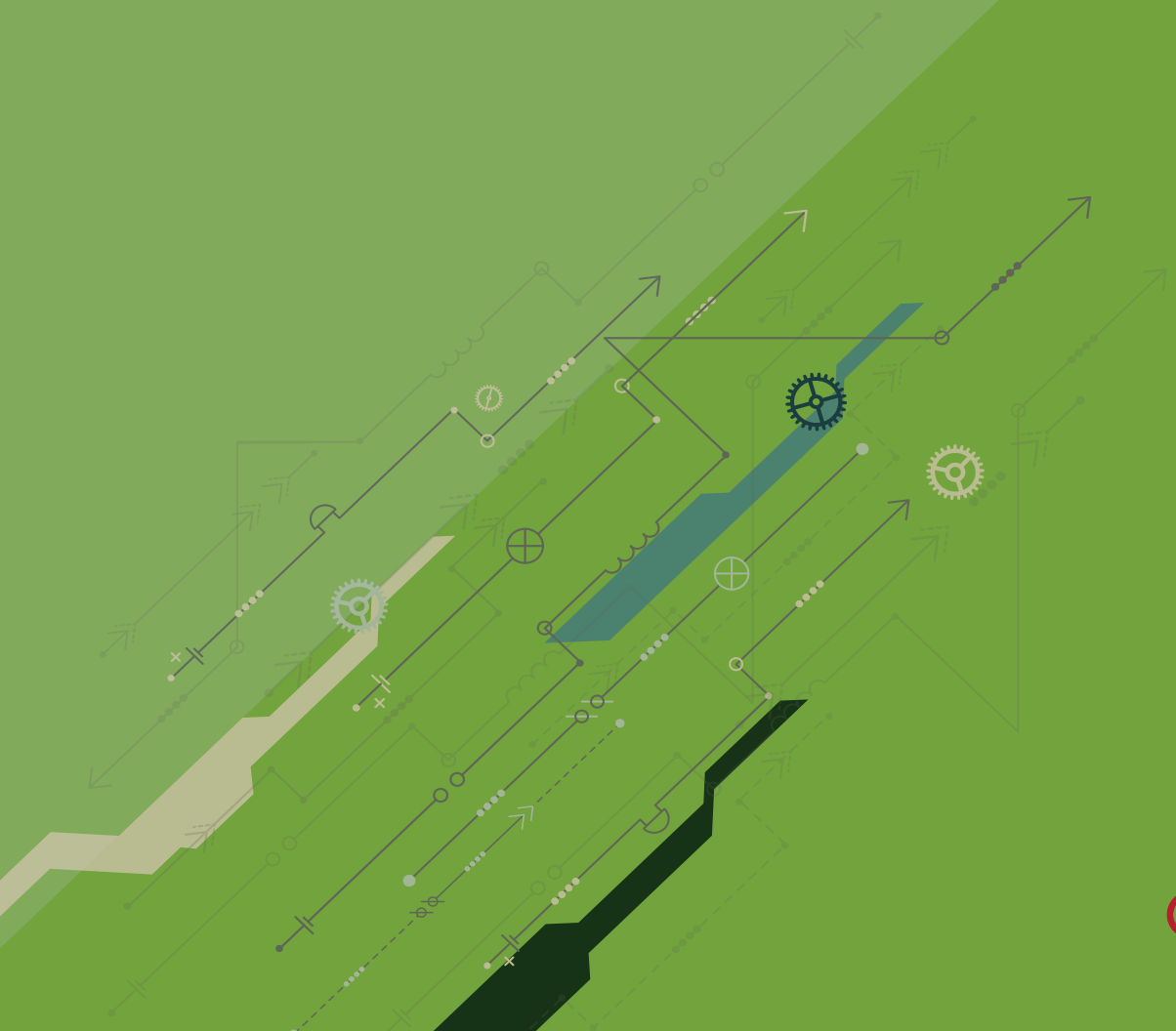
1% of systems has an exposed administration console or API interface (over HTTP/HTTPS)

Anonymous FTP: 1080 services detected (< 1%)

SAMPLE OF 2 MILLION ENDPOINTS

Protocol/Port	# of Ports discovered	% of exposed services
SSH	49,801	2.49%
PostgreSQL	40,012	2.00%
FTP	38,602	1.93%
MySQL	23,402	1.17%
RDP	14,603	0.73%
MSSQL	8,601	0.43%
RPC	3,503	0.18%
SMB	1,010	0.05%
Telnet	1,002	0.05%
PervasiveSQL	987	0.05%
Oracle	909	0.05%
Total of all Ports discovered	**182,432**	**9.13%**

"API detection is becoming a strong requirement with the arrival of Open Banking/PSD2 and the 'API economy' ecosystem..."



SUMMARY

We hope that this year's report helps to provide an insight into the types of issues we are finding, based on delivering thousands of security assessments every month, across multiple industry verticals.

With some focus being applied to some of the items highlighted, this should help any organisation maintain and improve their security posture.

VULNERABLE CODE

Given that the majority of vulnerabilities are still discovered in the web application layer, more focus needs to be placed on secure application development and continuous assessment, in order to keep pace with rapid deployment which is becoming more common.

CONTINUOUS VISIBILITY

It is not difficult to mitigate services that are exposed in error. The challenge is to maintain visibility and observe change, which leads to constant situational awareness. The ability to be alerted on change, is a key component especially in a rapidly changing landscape.

What's secure today may not be secure tomorrow and even if your systems do not change frequently, the world around you does, which may give rise to additional risks.

EXPOSED SERVICES

The exposure of sensitive or exploitable services simply increases ones "attack surface". It is simple logic that the less you have exposed to potential threat actors, the less likelihood of a security incident.

Deployment security needs to be considered such that only services you intend to be interacted with, are freely available to interact with on the public Internet.

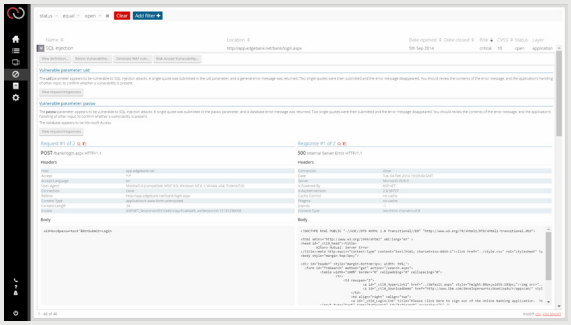
MALWARE EXPLOITING KNOWN VULNERABILITIES

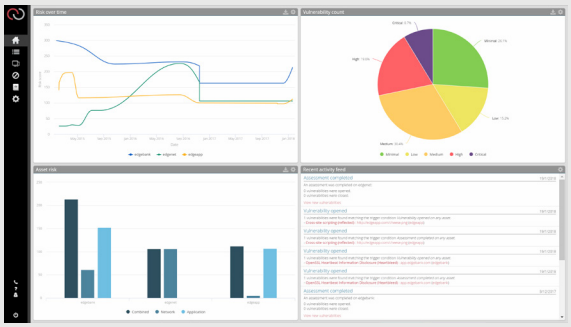
Most malware leverages known vulnerabilities (CVE's). These are vulnerabilities for which we have a fix for but the systems are still found to be vulnerable. For both internal and externally facing systems, discovery of vulnerabilities and systems which need patching is a must.

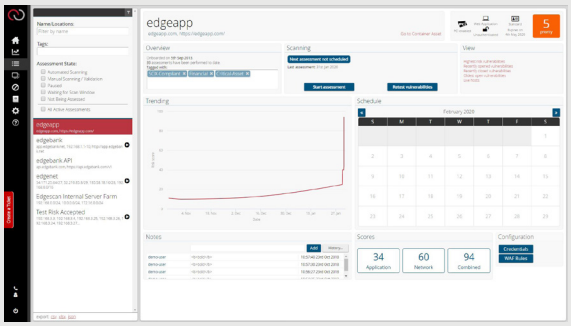
In some cases the vulnerability is not a high or critical risk CVE, but is a point of exploitation for malware to proliferate. Frequent CVE detection and control over ingress and egress traffic is core to improving malware resilience. Segmentation of systems in relation to criticality and data centric security zones is also worth considering if possible.

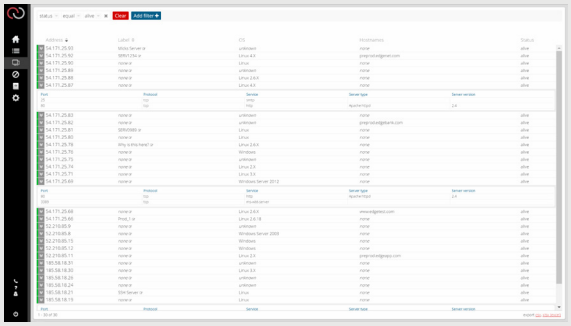
© 2020. BCC Risk Advisory Ltd.

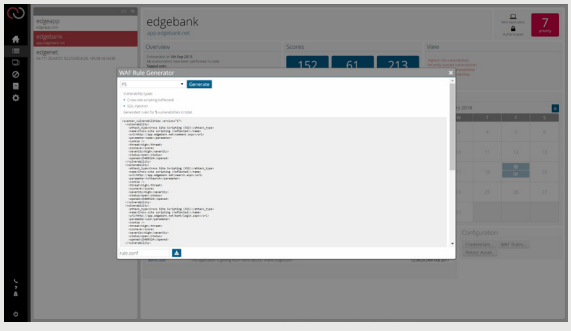
Edgescan **Portal**











ABOUT EDGESCAN

SaaS: Edgescan is a 'Security-as-a-Service (SaaS)' vulnerability management service which detects vulnerabilities in both web application and hosting infrastructure alike.

Hybrid Scalable Assessments: Edgescan detects both known (CVE) vulnerabilities and also web application vulnerabilities unique to the application being assessed due to our hybrid approach.

Analytics & Depth: Coupling leading edge risk analytics, production-safe automation and human intelligence, Edgescan provides deep authenticated and unauthenticated vulnerability assessment across all layers of a systems technical stack. Historical data to measure your risk profile over time. Effortless visibility into your fullstack security posture at-a-glance – Vulnerability Intelligence.

Coverage: Edgescan provides "fullstack vulnerability management" covering both hosting environments, component & frameworks and developer-written code. Our **edgescan advanced™** license even covers business logic and advanced manual testing techniques.

API Discovery & Assessment: Edgescan's API Scanner is able to detect vulnerabilities in any API, such as mobile back-end servers, IoT devices, and any RESTful APIs. Consume API descriptor files (Swagger, JSON, WSDL, YAML) and automatically test documented methods. Deliver API discovery profiling to help you maintain an asset register of APIs live on your estate. Discover APIs across your IP/CIDR ranges using our multi-layer API discovery technology – Find rogue or unknown APIs across your estate and alert you to new discoveries.

Support: Dedicated expert support from seasoned penetration testers and developers, to provide advice and remediation guidance.

Intelligent Validation: All vulnerabilities discovered by Edgescan are verified by our technology coupled with expert human analysis. This ensures accuracy. We eliminate false positives and streamline the remediation process, saving valuable developer time and resources.

Rich API Integration: Our API makes it simple to plug Edgescan into your ecosystem in order to correlate and reconcile, providing integration with both GRC and Bug Tracking and DevSecOps Systems alike.

Alerting: Customise Alerting via email, SMS, Webhooks, Slack, API etc, based on custom criteria.

Continuous Asset Profiling: Continuous profiling of the entire Internet-facing estate detecting changes in estate profile and eliminating blind spots.

Scale: Managing estates from one web application to thousands, from a single hosting environment to global cloud infrastructure, Edgescan delivers continuous vulnerability intelligence, support and testing-on-demand.

Compliance: Edgescan is a certified PCI ASV, ISO 27001 & CREST certified and delivers testing covering the OWASP Top 10, WASC threat classification, CWE/SANS Top 25, etc.

On-demand: Via the portal or API, request retests, ad-hoc scans as much as you need at no extra cost. All with the added comfort of validated findings and expert support.

Gartner SECURITY TOP 10 VULNERABILITY MANAGEMENT SOLUTION PROVIDERS - 2019 aws partner network PCI Security Standards Council APPROVED SCANNING VENDOR Contributor ISO 27001 CERTIFICATION EUROPE CREST Computing Security Awards WINNER The Irish Advantage

edgescan™

FULLSTACK VULNERABILITY MANAGEMENT™

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

Sales and general enquiries:
sales@edgescan.com

@edgescan

www.edgescan.com