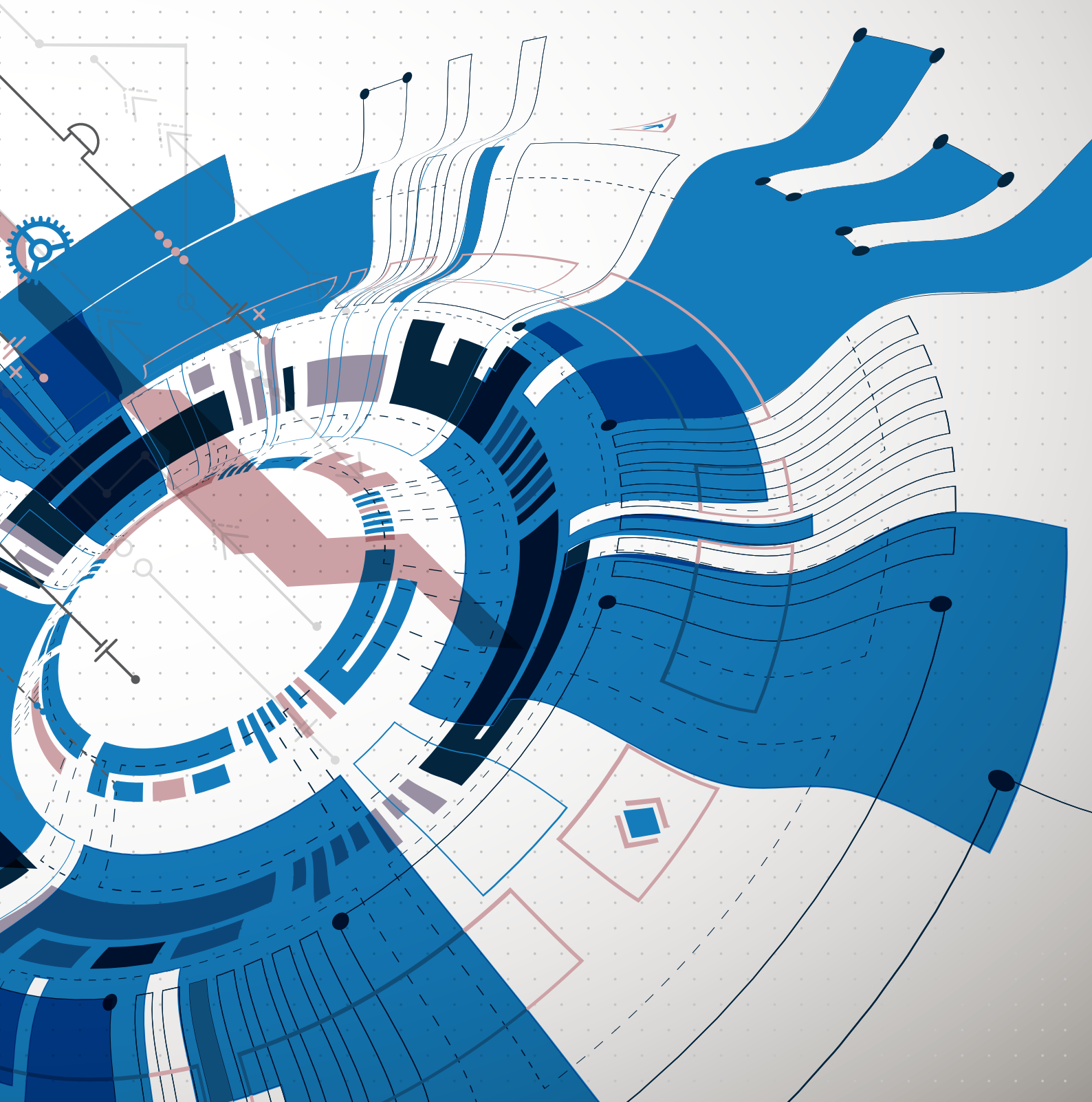
edgescan™

2019
VULNERABILITY STATISTICS REPORT



WELCOME

For our 4th Year running, welcome to the edgescan Vulnerability Stats Report. This report aims to demonstrate the state of full stack security based on edgescan data for 2018. 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. We still see high rates of known/patchable vulnerabilities which have working exploits in the wild, which possibly demonstrates it is hard to patch production systems effectively on a consistent basis.

Other metrics such as time-to-fix and risk density, still show that it takes time to fix vulnerabilities and it can be difficult to avoid repeating the same mistakes.

Visibility is also 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 and inform them of the exposure.

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, which leverage common vulnerabilities in corporate networks to spread across the enterprise.

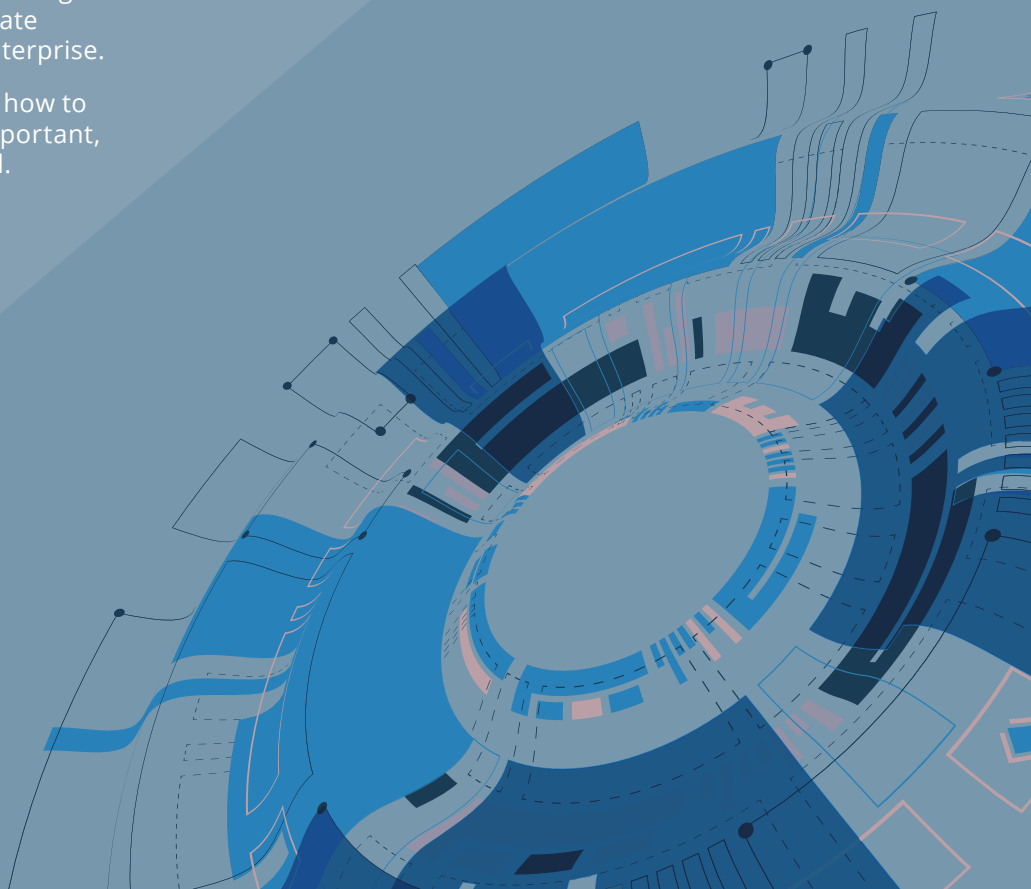
This report provides a glimpse of how to prioritize and focus on what is important, as not all vulnerabilities are equal.

Best regards,

Eoin Keary

EOIN KEARY

Founder,
Edgescan.com



edgescan™

2018 – A REVIEW

The pace of system development is now faster than ever, with deployment of systems in the cloud, DevOps and the world in continuous change. Overall a primary aspect of maintaining a robust and secure enterprise is Visibility.

Once we know that we have an issue, we generally act upon it. Based on this years findings, we still do not demonstrate strong situational awareness.

With the introduction of GDPR (25th May 2018), it is now clearer than ever that security breaches and non-compliance will result in tangible costs to an organisation. Protection of Personal Identifiable Information (PII) and sensitive data is now a serious requirement with regulatory penalties which could significantly damage any company. Other regulations such as NIS (Network and Information Systems Directive) drive the requirements for strong, repeatable and measurable cyber security controls.

2018 was (another) year of the data breach, from airlines to health insurers, from telecommunications companies to traditional industries such as hotel chains and retail organisations, all of which reported breaches. Some of these were via malware and others via hacking attacks, but there is no sign of this level of global breach slowing in 2019. The bottom line is that a simple vulnerability or the absence of a simple control can result in catastrophic results.

Many breaches via hacking attacks and malware are preventable. Activities such as security integration into the SDLC, DevSecOps, patch management, continuous vulnerability management and continuous asset profiling (i.e. visibility), can help us identify and mitigate such weaknesses before we deploy systems, or at least before they become a real problem.

DevSecOps Toolchain Integration is commonplace and still gaining traction, which is an effective way to detect vulnerabilities in developed code and systems without slowing down output. Some caveats exist with such approaches, such as accuracy, coverage and business logic assessment, when using a purely automated solution, but simple common high-risk vulnerabilities can be detected quickly and mitigated quickly when combining human intelligence and “tuned” automation.

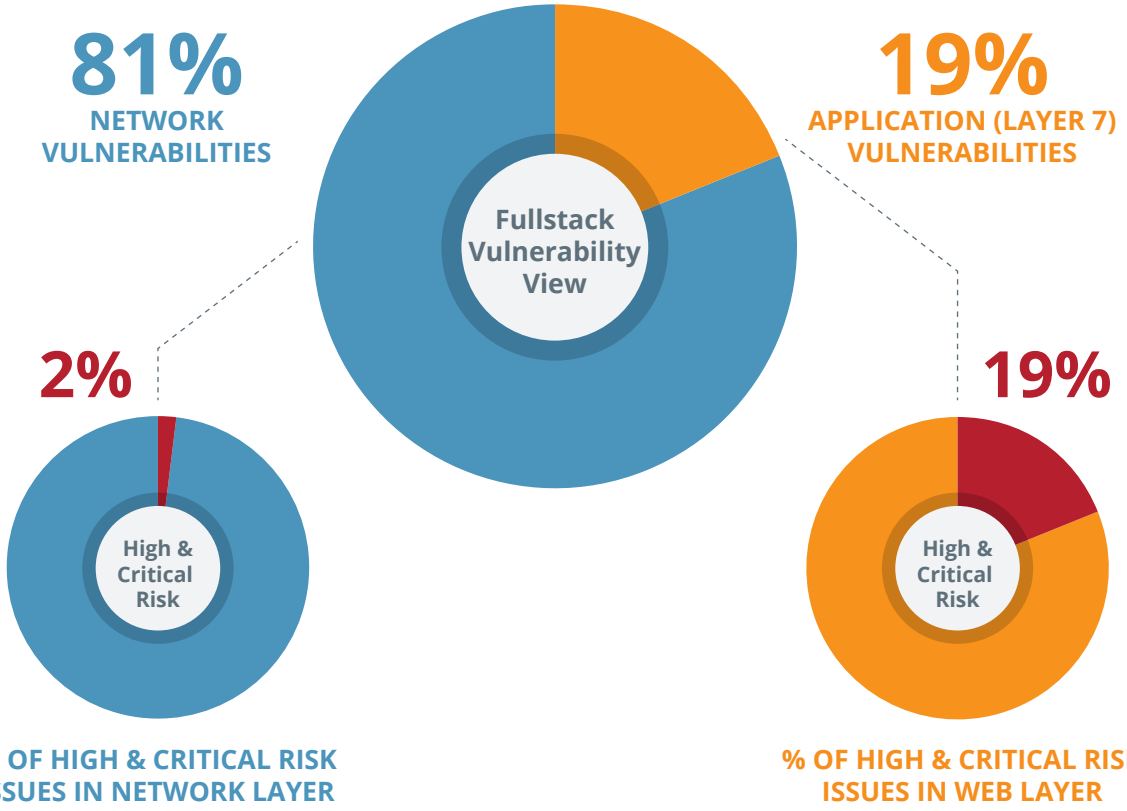
Many people find the output of security tools overwhelming due to the volume and inaccuracy of data presented. This needs to be addressed so developers and system deployment teams can focus and prioritise on risks which matter to the enterprise. As the saying goes “Not all vulnerabilities are created equal”.

The world of the “annual pentest” is dead. We deploy code and systems too frequently and too rapidly for traditional approaches to cyber security to keep pace with any meaningful effect on overall security posture. As an industry we should embrace more automation coupled with human expertise to augment our capabilities as professionals and become somewhat “bionic”.

edgescan™ January 2019

RISK DENSITY – INFRASTRUCTURE VS LAYER 7

In 2018 we discovered that on average, 19% of all vulnerabilities were associated with (Layer 7) web applications, API's, etc., and 81% were network vulnerabilities.



- The Risk Density is still high and has not changed significantly from last years report.
- Even though we find more vulnerabilities in the infrastructure layer, the application layer is where we find a higher degree of risk. This is due to the "snowflake effect" – every application is unique, developed in a stand-alone fashion and serves a unique purpose, as opposed to infrastructure which is commoditised and much more uniform.
- Change and uniqueness certainly introduces additional risk.
- Internal, non-public application layer security is worse – 24.9% of all discovered vulnerabilities are High or Critical Risk.

RISK DENSITY – NETWORK VS APP

Web Application security is still the area of most risk from a security breach standpoint. This year we have introduced both public Internet and internal network views of the vulnerability management landscape.

The percentage of High and Critical risks combined, compared to all discovered risks is still high at 19.2% for public Internet-facing (external) applications and 24.9% for non-public or internal applications.

This compares to a risk density of 20.7% for Internet-facing systems last year, which is roughly similar.

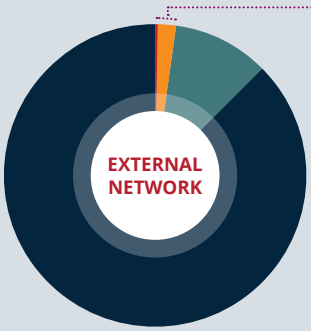
The high-risk density score of 24.3% for internal-facing applications is worrisome given many studies cite the "insider threat" as a significant issue. Malware and ransomware also target known vulnerabilities and can easily exploit internal systems, should they get the opportunity to do so.

High and Critical Risk Density in Internet-facing (external) Infrastructure is still relatively low at 2% whilst internal infrastructure risk density is higher, at 4.2%.

RISK DENSITY

EXTERNAL – NET

0.2% CRITICAL
1.8% HIGH
10.2% MEDIUM
87.8% LOW

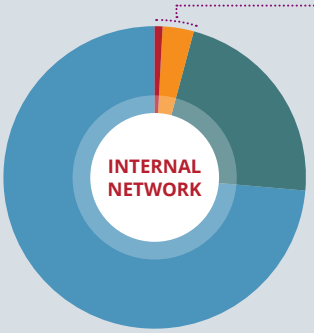


2% OF ALL VULNERABILITIES DISCOVERED WERE HIGH OR CRITICAL RISK

10.2% OF ALL VULNERABILITIES DISCOVERED WERE MEDIUM RISK

INTERNAL – NET

0.8% CRITICAL
3.4% HIGH
22.2% MEDIUM
73.5% LOW

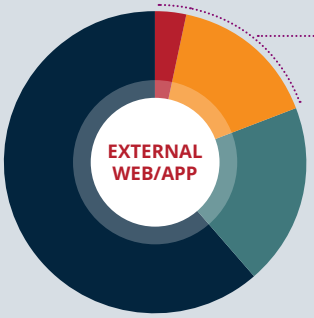


4.2% OF ALL VULNERABILITIES DISCOVERED WERE HIGH OR CRITICAL RISK

22.2% OF ALL VULNERABILITIES DISCOVERED WERE MEDIUM RISK

EXTERNAL – WEB

3.4% CRITICAL
15.8% HIGH
19.4% MEDIUM
61.4% LOW

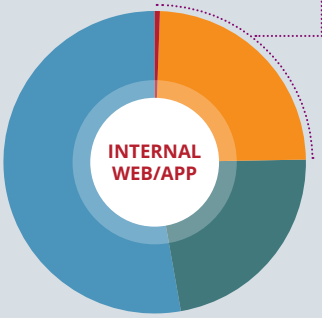


19.2% OF ALL VULNERABILITIES DISCOVERED WERE HIGH OR CRITICAL RISK

19.4% OF ALL VULNERABILITIES DISCOVERED WERE MEDIUM RISK

INTERNAL – WEB

0.6% CRITICAL
24.3% HIGH
22.5% MEDIUM
52.8% LOW



24.9% OF ALL VULNERABILITIES DISCOVERED WERE HIGH OR CRITICAL RISK

22.5% OF ALL VULNERABILITIES DISCOVERED WERE MEDIUM RISK

VULNERABILITY TAXONOMY

Previously we have discussed the rates of vulnerability across both Web Applications and Hosting environments. What is also interesting is to delve into what type of vulnerabilities are being discovered. The following is a high level breakdown of the types of issues being identified by edgescan™.

Below Layer 7

From a Host/Network perspective we still see a large % of issues are related to Cryptography which covers issues such as deprecated protocol support, CVE's and poor implementation.

Weak configuration also gives rise to a significant percentage of discovered vulnerabilities.

Layer 7

From an application security standpoint, insecure configuration is also a significant issue, followed by client-side security. Injection attacks are also relatively high given how destructive they can be.

MOST COMMON INFRASTRUCTURE VULNERABILITIES IN 2018

- Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cyber security vulnerabilities.
- Many systems have a CVE which defines a security issue that is known to the public. Generally there is a patch or workaround available to mitigate the issue.
- Systems with exposed CVE's generally are not being patched regularly. It takes time and effort to patch, but it appears patching can still reduce ones exposure to breaches and significantly increase security.
- CVE's (Known Vulnerabilities) can be detected quickly using a continuous assessment model. Even though your source code does not change, a vulnerability may be discovered which was previously unknown within the security industry and may require your attention.
- Continuous visibility and real-time alerting is the key to detecting CVE's.

MOST COMMON INFRASTRUCTURE VULNERABILITIES IN 2018

1.29%
FIREWALL UDP PACKET SOURCE PORT 53 RULESET BYPASS

Bypass of firewall rules by sending UDP packets with a source port equal to 53

E.g. CVE-2003-1491, CVE-2004-1473

1.18%
MICROSOFT WINDOWS SMB NULL SESSION AUTHENTICATION

A server with Microsoft Windows where is it possible to log into it using a NULL session

E.g. No login ID or password requred. CVE-1999-0519, CVE-1999-0520, CVE-2002-1117

0.82%
SNMP AGENT DEFAULT COMMUNITY NAME (PUBLIC)

An attacker may be able to use information to gain more knowledge about the remote system or change the configuration settings (if the default community allow such modifications).

E.g. CVE-1999-0517

44.7%
TLS & SSL VERSION & CONFIGURATION ISSUES

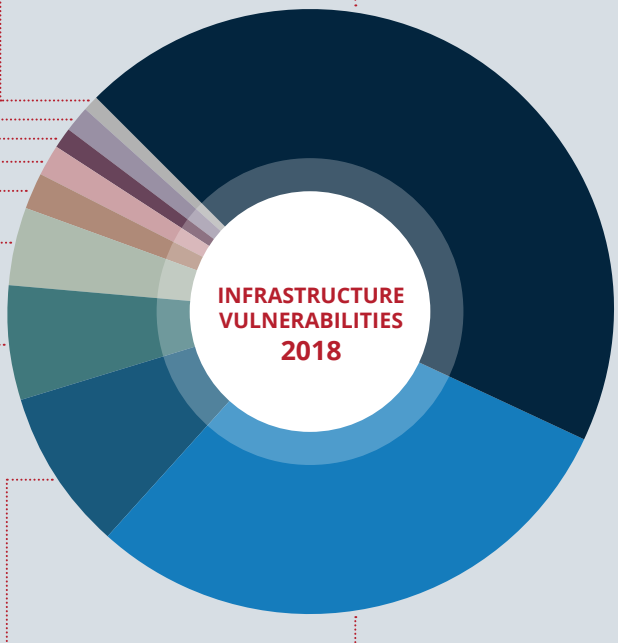
Unsupported versions of SSL/ TLS enabled. Weak ciphers used. Vulnerabilities to known SSL CVE's detected. SSL Certificate expiry or "bad" certificates.

1.69%
UNSUPPORTED & UNPATCHED SERVER DETECTION

Unpatched, unsupported servers both *nix and Windows. 1000's of CVE's recorded against them as a result.

1.78%
RETURN OF BLEICHENBACHER'S ORACLE THREAT (ROBOT) INFORMATION DISCLOSURE

An adaptive-chosen ciphertext attack: this attack fully breaks the confidentiality of TLS when used with RSA encryption.



4.15%
UNENCRYPTED TELNET SERVICES

Insecure and unencrypted protocol for data transfer.

6.25%
WINDOWS REMOTE DESKTOP PROTOCOL SERVER MAN-IN-THE-MIDDLE

CVE's such as CVE-2005-1794, CVE-2014-0296, CVE-2015-2472, CVE-2012-0002, CVE-2012-0152

8.61%
OpenSSH MULTIPLE VULNERABILITIES & CONFIGURATION ISSUES

Issues such as SSH Weak MAC Algorithms Enabled, SSH Server CBC Mode Ciphers Enabled, Exposed SSH service.

E.g. CVE-2018-15473, CVE-2016-6210, CVE-2016-6515

29.53%
SMB SECURITY ISSUES

SMB authentication, known vulnerabilities, etc.

As per previous years, TLS, SSL issues top the most common list at 44.7%

SMB security issues are also significant and are related to various mass malware attacks in 2018

RDP (Remote Desktop) vulnerabilities were also relatively common and are a popular target for attackers according to 2018 threat intel

MOST COMMON WEB (LAYER 7) VULNERABILITIES

14.69%
CROSS SITE SCRIPTING/ BROWSER SINK ATTACKS

HTML Injection, Stored and Reflected Cross-Site Scripting. Template Injection. Generally found due to a lack of or poor contextual output encoding.

12.36%
VULNERABLE COMPONENTS

Unpatched, unmanaged, known CVE (vulnerability). Misconfigured components and insecure defaults.

9.25%
WEAK AUTHENTICATION

Weak passwords, Enumeration/ Leakage, Error related issues.

8.18%
OTHER INJECTION (OS, CRLF, HTTP, XXE)

Injection attacks, Operating system, Backend injection. Pivoting attacks, Command Shell and stepping stone attacks to assist in total compromise of hosting environment and associated network.

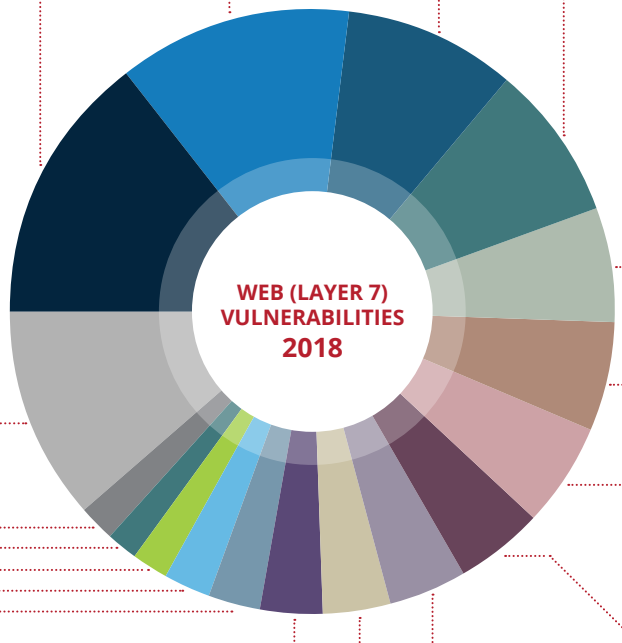
11.34%
OTHER

6.3%
EXTERNAL SERVICE INTERACTION

Forceful control of target to interact with external system. When it is possible to induce an application to interact with an arbitrary external service.

1.75%
CROSS SITE REQUEST FORGERY

An attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.



5.72%
SOURCE CODE DISCLOSURE

Backend source code disclosure due to error or poor application design.

1.78%
SESSION HANDLING WEAKNESS

Session management weaknesses.

5.55%
SQL INJECTION (& LDAP INJECTION)

Database attack via vulnerable web application.

1.82%
DOM BASED VULNERABILITY

Client-side browser attacks, Javascript attacks

4.62%
SYSTEM EXPOSURE

Exposed Admin Console, Directory traversal, Insecure configuration exposure, Insecure defaults.

2.53%
OPEN REDIRECTION

Web application accepts untrusted input that could cause the web application to redirect the request to a URL contained within untrusted input.

2.81%
AUTHORISATION ISSUE

Unauthorised data & functional access weakness. Privilege escalation, horizontal and vertical authorisation weakness.

3.32%
INFORMATION DISCLOSURE/ERROR HANDLING

Sensitive information & System information disclosure. Poor error handling.

3.6%
SENSITIVE INFORMATION DISCLOSURE

Sensitive business information, PII, Credentials, etc.

4.38%
MALICIOUS FILE UPLOAD

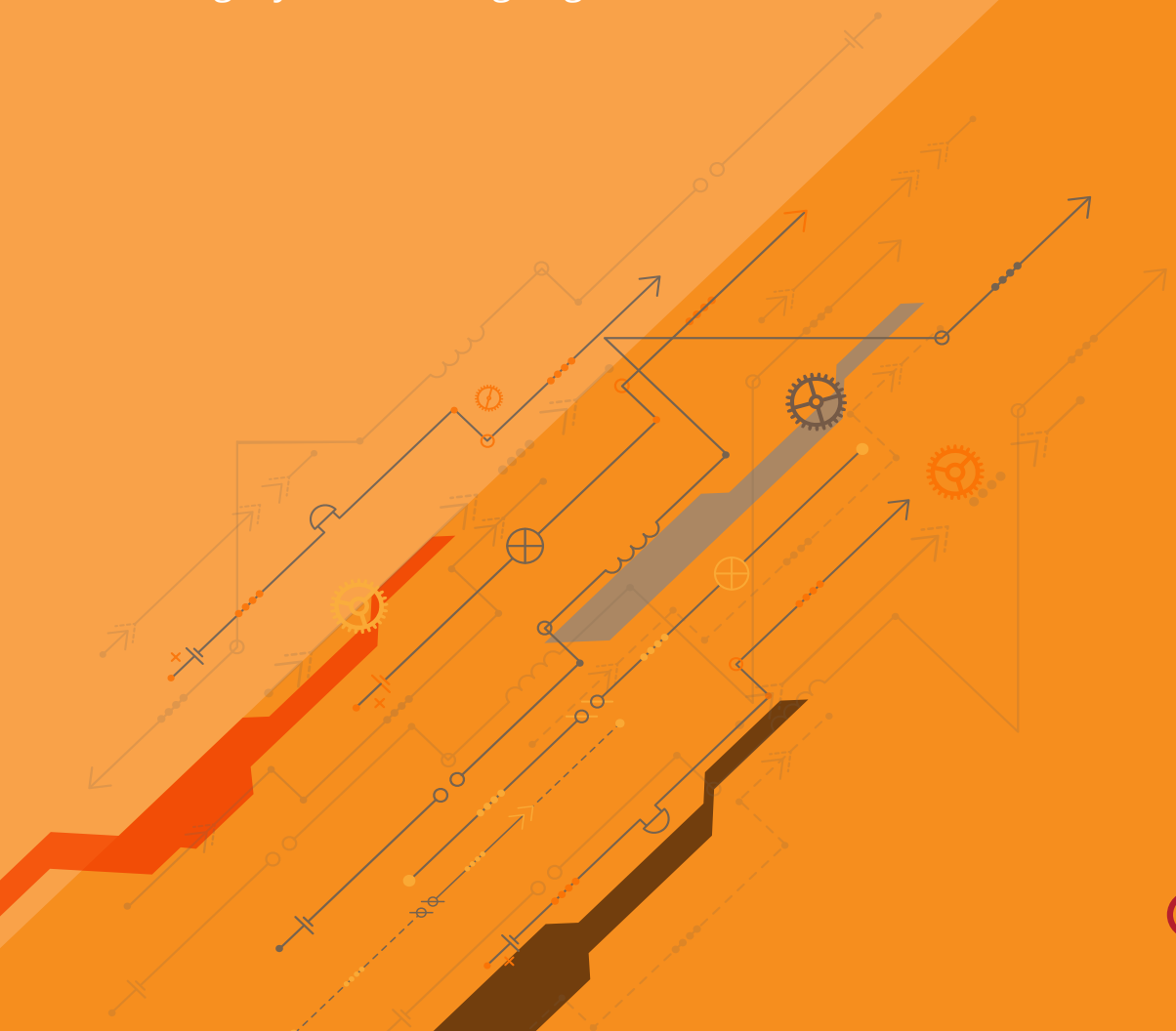
Successfully upload malicious payload to target. No antivirus or poor handling of untrusted payloads.

Cross-Site Scripting, both reflected and stored, was the most common vulnerability in 2018 at 14.69%.

Vulnerable components were significant in 2018 at 12.36%, which begs the question of the extent to which organisations are managing software component inventory and bill-of-materials. Many of the vulnerable components had known vulnerabilities with working exploits available.

SQL Injection was also significant in 2018 at 5.55%, in terms of how devastating the attack can be and how easily it can be used to exploit entire systems.

Other Injection attacks such as OS, CRLF, JavaScript, backend and template attacks were high in 2018 at 8.18%. Many of these vulnerabilities could result in significant data/PII loss or attacks on audit integrity controls (e.g. logs).



MOST COMMON CVE'S – EXTERNAL
(EXCLUDING SSL RELATED ISSUES)

MOST COMMON HIGH AND CRITICAL CVE'S IN PUBLIC INTERNET FACING SYSTEMS

The following depicts the most common High and Critical Risk CVE's discovered in the 12 months to December 2018 for public Internet facing systems. It excludes SSL/TLS related issues due to the volume of issues, which tends to skew the overall results.

The "NotPetya" ransomware variant utilized in the 2017 attack uses EternalBlue, an exploit which takes advantage of a vulnerability in Windows' Server Message Block (SMB) protocol. EternalBlue is generally believed to have been developed by the U.S. National Security Agency (NSA); it was leaked in April 2017 and was also used by WannaCry.

7.5% of all high and critical risk vulnerabilities discovered in 2018 related to exposure to NotPetya CVE's (CVE-2017-0144, CVE-2017-0145) - Windows SMB Remote Code Execution Vulnerability

33.33% of all high and critical risk vulnerabilities discovered in 2018 were in relation to unsupported Windows Server 2003 systems (no patching, support, end-of-life systems)

Systems running PHP and Apache also contributed to the Top 10 due to weak component security and traditional patch management of exposed systems

Name	% of all total discovered	CVSS Score	CVE's
Microsoft Windows Server 2003 Unsupported system	33.33%	10	CVE-2005-0416, CVE-2005-3483, CVE-2006-2373, CVE-2006-2374, CVE-2007-0038, CVE-2007-1765, CVE-2008-0015, CVE-2008-0020, CVE-2009-1923, CVE-2009-1924, CVE-2009-3675, CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231, CVE-2010-1886, CVE-2015-1768,CVE-2015-1768
MS14-066: Vulnerability in Schannel – Remote Code Execution	7.53%	10	CVE-2014-6321
MS15-034: Vulnerability in HTTP.sys – Remote Code Execution	7.53%	10	CVE-2015-1635
MS17-010: Security Update for Microsoft Windows SMB Server ETERNALBLUE WannaCry Petya	7.53%	9.3	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,CVE-2017-0148
Microsoft Windows SMBv1 Various Vulnerabilities	6.45%	9.3	CVE-2017-0267, CVE-2017-0268, CVE-2017-0269, CVE-2017-0270, CVE-2017-0271, CVE-2017-0272, CVE-2017-0273, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279,CVE-2017-0280
PHP 5.6.x < 5.6.33 Various Vulnerabilities	6.45%	10	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-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, 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, CVE-2016-9935, CVE-2017-11142, CVE-2017-11143, CVE-2017-11144, CVE-2017-11145, CVE-2017-6004, CVE-2017-7890, CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, CVE-2017-9229, CVE-2018-5711, CVE-2018-5712
Apache Traffic Server 4.x < 4.2.1.1 / 5.x < 5.0.1 Synthetic Health Check Vulnerability	4.30%	10	CVE-2014-3525
Dropbear SSH Server < 2016.72 Various Vulnerabilities	3.23%	10	CVE-2016-7406, CVE-2016-7407, CVE-2016-7408, CVE-2016-7409
HP Data Protector - Command Execution	3.23%	10	CVE-2011-0923
MS12-020: Vulnerabilities in RDP – Remote Code Execution	3.23%	9.3	CVE-2012-0002, CVE-2012-0152
Other	17.20%		

MOST COMMON CVE'S – INTERNAL
(EXCLUDING SSL RELATED ISSUES)

MOST COMMON HIGH AND CRITICAL RISK INTERNAL NETWORK CVE'S

The following depicts the most common High and Critical Risk CVE's discovered in the 12 months to December 2018 for internal (non public Internet) network systems.

5.23% of all discovered high and critical vulnerabilities discovered related to exposure to NotPetya, Wannacry, Eternalblue CVE's

8.76% of all discovered high and critical risk vulnerabilities related to unpatched windows 2003 systems which have a significant list of known vulnerabilities

Internal security has always been considered the "Soft underbelly" in network security. Given the spate of Ransomware and Malware attacks which occurred in 2018, the successful release of such malware would cause significant harm due to unpatched and poorly managed non Internet facing systems.

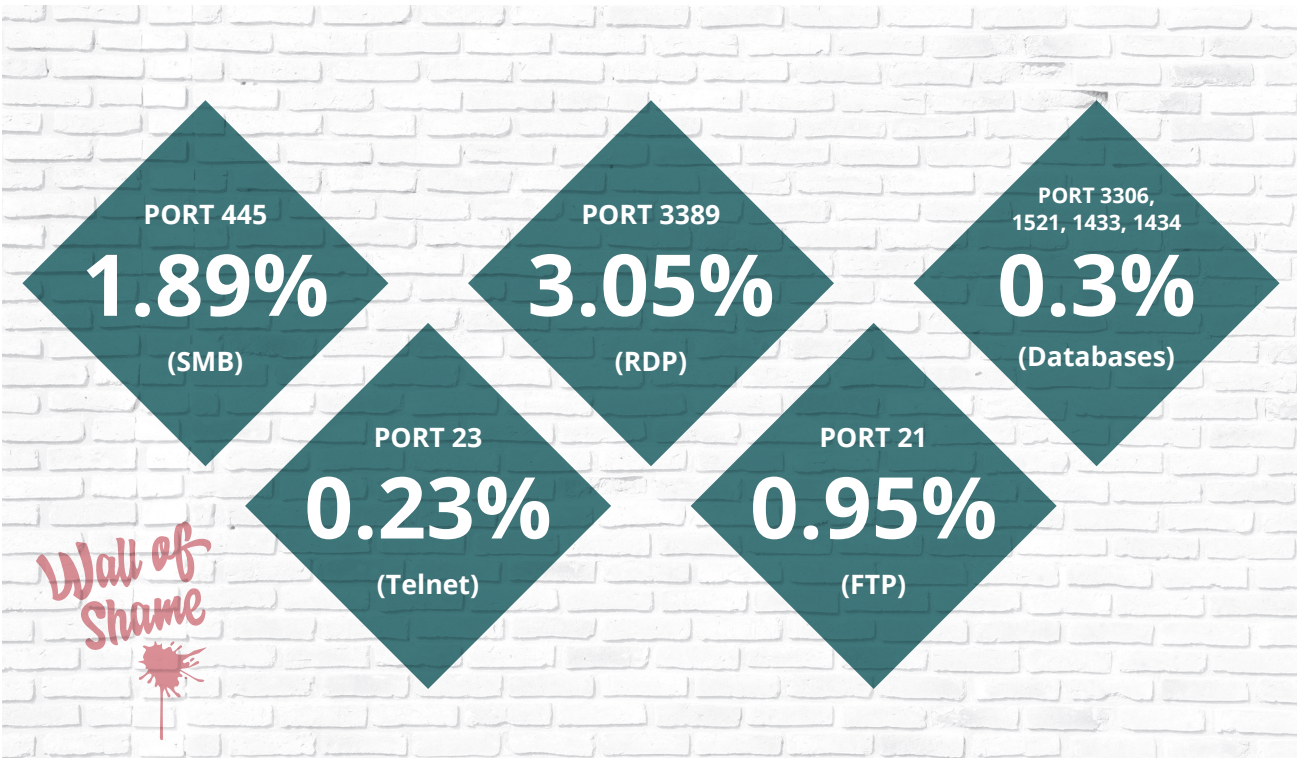
Name	% of all total discovered	CVSS Score	CVE's
Microsoft Windows SMBv1 Vulnerabilities	11.40%	9.3	CVE-2017-0267, CVE-2017-0268, CVE-2017-0269, CVE-2017-0270, CVE-2017-0271, CVE-2017-0272, CVE-2017-0273, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279, CVE-2017-0280
MS12-020: Vulnerabilities in Remote Desktop - RCE	10.30%	9.3	CVE-2012-0002,CVE-2012-0152
HP System Management Homepage < 6.3 Various Vulnerabilities	9.36%	10	CVE-2010-1917, CVE-2010-2531, CVE-2010-2939, CVE-2010-2950, CVE-2010-3709, CVE-2010-4008, CVE-2010-4156, CVE-2011-1540, CVE-2011-1541
Microsoft Windows Server 2003 Unsupported Installation Detection	8.76%	10	CVE-2005-0416, CVE-2005-3483, CVE-2006-2373, CVE-2006-2374, CVE-2007-0038, CVE-2007-1765, CVE-2008-0015, CVE-2008-0020, CVE-2009-1923, CVE-2009-1924, CVE-2009-3675, CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231, CVE-2010-1886, CVE-2015-1768, CVE-2015-1768
HP Data Protector - Command Execution	5.84%	10	CVE-2011-0923
MS17-010: Security Update for Microsoft SMB Server – ETERNALBLUE, WannaCry, EternalRocks, Petya	5.23%	10	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
MS14-066: Vulnerability in Schannel - RCE	4.90%	10	CVE-2014-6321
HP Data Protector Remote Command Execution	4.74%	10	CVE-2011-0923
HP System Management Homepage < 7.6.1 Various Vulnerabilities (HPSBMU03753)	2.48%	7.8	CVE-2016-8743, CVE-2017-12544, CVE-2017-12545, CVE-2017-12546, CVE-2017-12547, CVE-2017-12548, CVE-2017-12549, CVE-2017-12550, CVE-2017-12551, CVE-2017-12552, CVE-2017-12553
MS15-011: Vulnerability in Group Policy – RCE (3000483)	1.98%	8.3	CVE-2015-0008
Other	35.20%		

EXPOSED SERVICES:
ASSET PROFILING – OPEN PORT WALL OF SHAME

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. Systems such as remote desktop, SMB, Database, Telnet etc.

Many exposed ports have been used for attacks such as WannaCry, NotPetya, Mirai, ADB Miner, PyRoMine amongst others. Such exposed ports can be victim to traditional hacking attacks which also give rise to breach and data loss.

Below depicts the percentage of systems facing the internet with exposed ports and services (Based on a sample of 250,000 assets under continuous profiling):



Remediation of this type of issue simply requires a firewall change or services being shut down. This sounds simple but the challenge is attaining visibility in the first place. Continuous asset profiling helps detect open services and when coupled with an alerting mechanism to notify one of an exposure, it is an easier challenge to address. Simply put, visibility helps reduce a systems attack surface, in a constantly changing environment.

(CONTINUED)

The table below depicts the most commonly found exposed ports, most of which should probably not be! These are based on a sample of 250,000 public Internet-facing assets under continuous profiling in the past 12 months to December 2018.

In total, 25.21% of all exposed ports as outlined in the table below, should likely be protected or further protection considered. The ports listed are frequently abused to commit a security breach or to help proliferate malware attacks.

Common ports such as Port 80 (HTTP) & Port 443 (HTTPS) are obviously not included	0.3% (750) exposed databases	3.05% (7,625) exposed RDP (Remote Login Services)	2.65% (6,500) exposed Redis services (Redis is an in-memory data structure store)

Protocol	Service Name/Description	% of all discovered open ports
tcp	SSH	7.7868%
tcp	RDP	3.0596%
udp	SNMP	2.6502%
tcp	redis	2.0100%
tcp	Microsoft RPC	1.9132%
tcp	SMB	1.8983%
tcp	NetBIOS Session Service	1.7569%
udp	ntp	1.5856%
tcp	FTP	0.9529%
tcp	DNS Firewall Port	0.7221%
tcp	Exposed Database	0.3059%
tcp	Telnet	0.2394%
tcp	DHCP Server	0.1773%
tcp	VNC	0.1507%
Total of all Ports discovered		**25.21%**

T2F (TIME TO FIX):
WEB APPLICATIONS & INFRASTRUCTURE

THE AVERAGE TIME TO FIX OR MITIGATE A VULNERABILITY DISCOVERED IN THE APPLICATION (WEB) AND INFRASTRUCTURE LAYERS

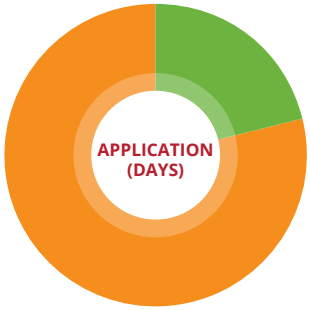
APPLICATION

69 DAYS
CRITICAL RISK

83 DAYS
HIGH RISK

74 DAYS
MEDIUM RISK

84 DAYS
LOW RISK/INFO



77.5
AVERAGE TIME TO CLOSE A VULNERABILITY IN NUMBER OF DAYS

TIME TO FIX CRITICAL

Shortest Time
1.25 Days

Longest Time
215 Days

TIME TO FIX HIGH

Shortest Time
3 Days

Longest Time
323 Days

TIME TO FIX MEDIUM

Shortest Time
0.2 Days

Longest Time
348 Days

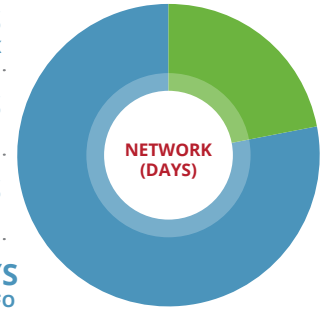
NETWORK

65 DAYS
CRITICAL RISK

64 DAYS
HIGH RISK

78 DAYS
MEDIUM RISK

120 DAYS
LOW RISK/INFO



81.75
AVERAGE TIME TO CLOSE A VULNERABILITY IN NUMBER OF DAYS

TIME TO FIX CRITICAL

Shortest Time
0.2 Days

Longest Time
198 Days

TIME TO FIX HIGH

Shortest Time
8.8 Days

Longest Time
256 Days

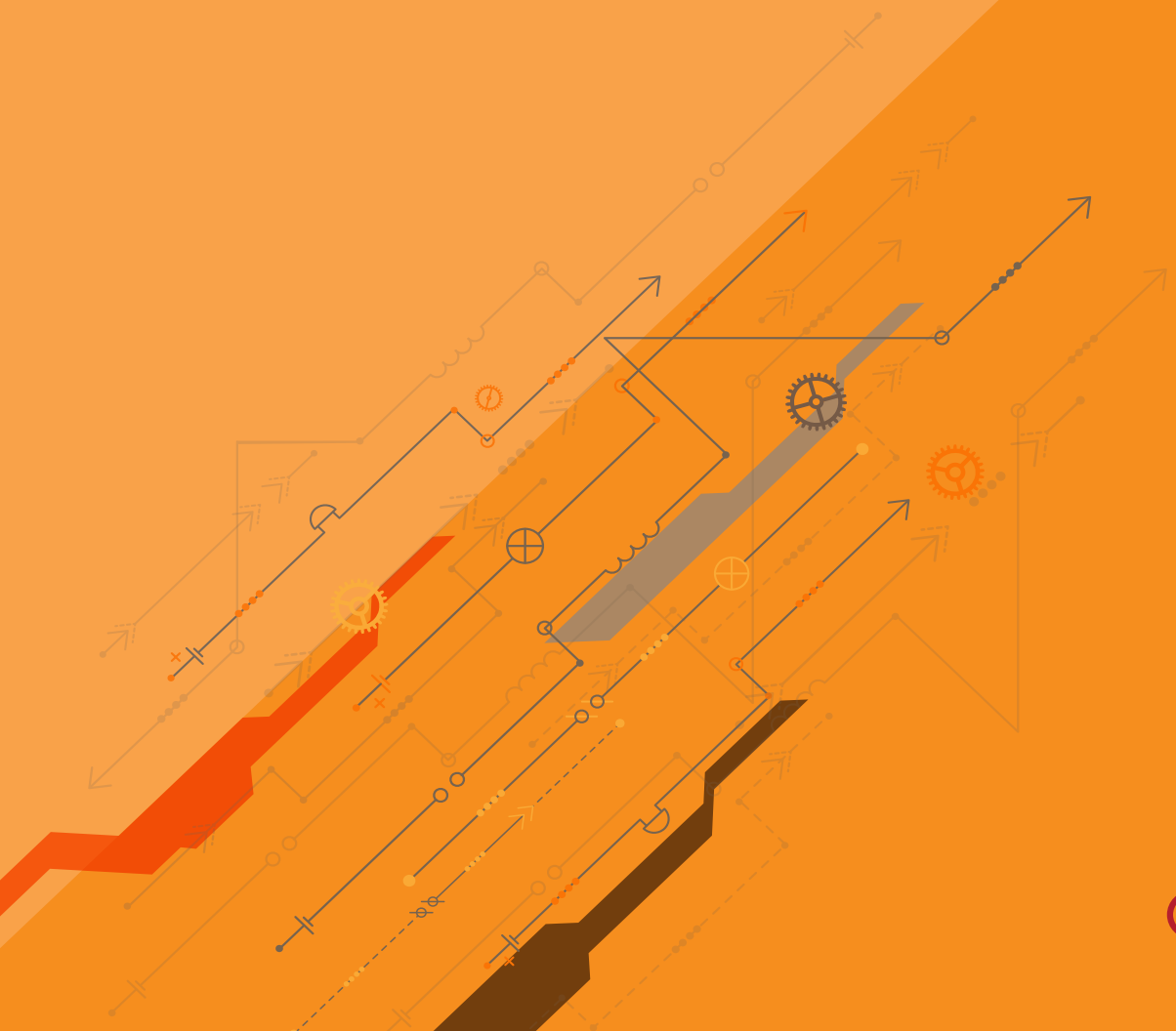
TIME TO FIX MEDIUM

Shortest Time
5.6 Days

Longest Time
345 Days

The average window of exposure for critical infrastructure vulnerabilities is 65 days

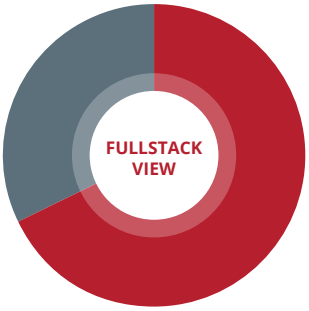
The average window of exposure for critical web application vulnerabilities is 69 days



PCI ASV VIEW

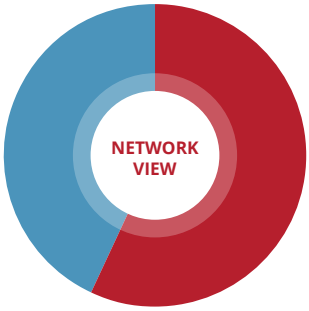
The Payment Card Industry Data Security Standard (PCI DSS) defines a vulnerability with a base CVSS score of 4.0 or greater, as a compliance Fail. edgescan™ is a certified PCI Approved Scanning Vendor (ASV) and assists clients with PCI DSS compliance by leveraging its full stack security assessment technology and technical support.

68%



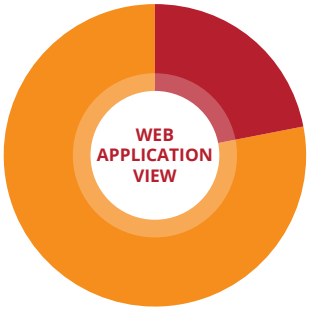
68% OF ALL VULNERABILITIES DISCOVERED IN 2018 HAD A SCORE EQUAL TO OR HIGHER THAN 4.0 – PCI DSS FAIL

57%



57% OF ALL NETWORK LAYER VULNERABILITIES DISCOVERED IN 2018 HAD A SCORE EQUAL TO OR HIGHER THAN 4.0 – PCI DSS FAIL

22%



22% OF ALL WEB APPLICATION VULNERABILITIES DISCOVERED IN 2018 HAD A SCORE EQUAL TO OR HIGHER THAN 4.0 – PCI DSS FAIL

Common Vulnerability Scoring System (CVSS) base score (http://www.first.org/cvss/), as indicated in the National Vulnerability Database (NVD) where applicable (http://nvd.nist.gov/cvss.cfm).

CVE – COMMON VULNERABILITIES AND EXPOSURES

HTTPS://CVE.MITRE.ORG/

Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cyber security vulnerabilities.

Many systems have a CVE which defines a security issues known to the public. Generally there is a workaround or a patch to mitigate this issue.

Systems with CVE's exposed generally are not being patched regularly. It takes time and effort to patch, but it appears patching can still reduce ones exposure to breach and increase security posture significantly.

CVE's (Known Vulnerabilities) can be detected quickly using a continuous assessment model. Even though your source code does not change, a vulnerability may be discovered which may require your attention; *Continuous visibility* is the key to detecting CVE's.

CVE LANDSCAPE

Oldest CVE in 2018: CVE-1999-0017

*"FTP servers can allow an attacker to connect to arbitrary ports on machines other than the FTP client, aka FTP bounce"**

CVSS: 7.5

Most Common in 2018: 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."

CVSS: 4.3

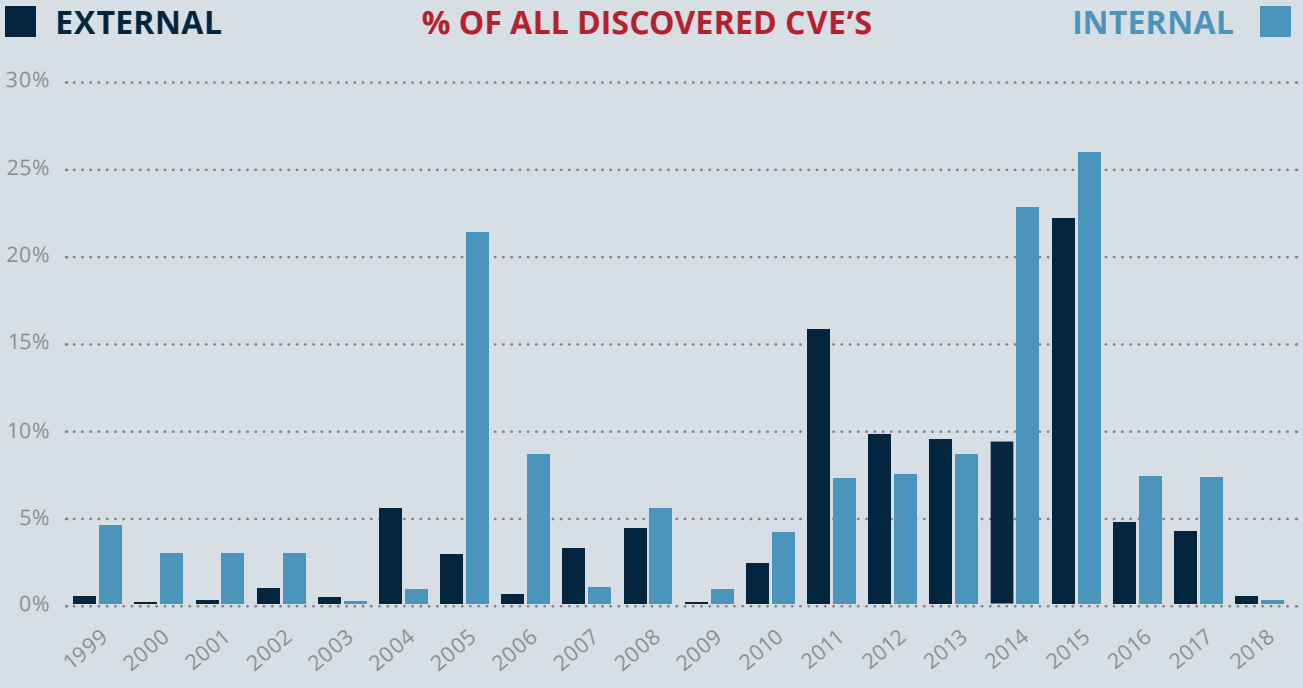
Systems with Multiple Vulnerabilities

81.58% of systems had at least one CVE

72.11% of systems had more than one CVE

Interestingly, 20.57% of systems had more than 10 CVEs

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



#ProTip: Patching and version maintenance is still a key part of maintaining a secure posture. Many systems have vulnerabilities which simply have not been discovered yet; once they are, a patch is usually available shortly after. It is recommended to keep pace with patching.

CONCLUSION

AWARENESS

Application security needs to become a board-level conversation in your organization, if it is not already.

MEASURE

Management sponsorship for application security should be result-oriented to help raise your organisations security posture.

REWARD

Rewarding of development teams and gamification, including metrics and measuring the security posture of businesses applications, should be considered.

CAPABILITY

Security champions need to have the resources and services they require to identify and fix vulnerabilities in software and supporting hosting environments faster.

BILL OF MATERIALS

Understand the composition of software applications and prioritize the vulnerable libraries and frameworks for your teams to maintain.

VISIBILITY

Improve situational awareness of your estate at any given time, helping mitigate even relatively simple issues. Move to a position of strong visibility as we cannot improve on what we do not know.

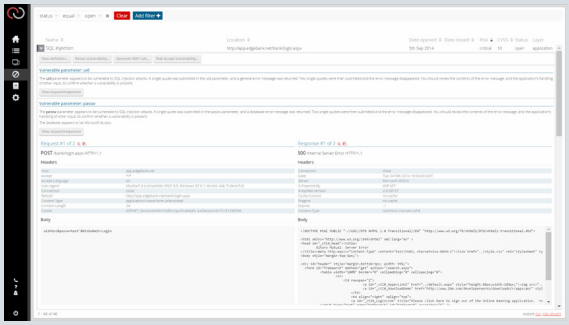
TEAM

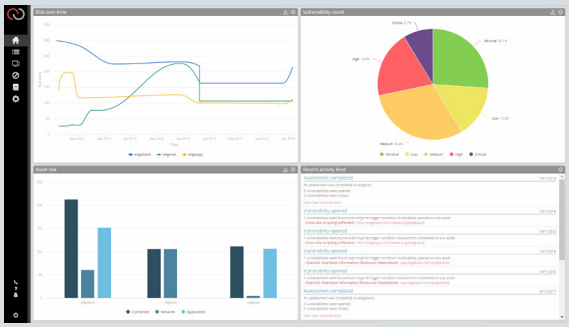
Work with IT and operations to apply scheduled maintenance windows, aimed at updating systems and frameworks with security patches using a risk based approach.

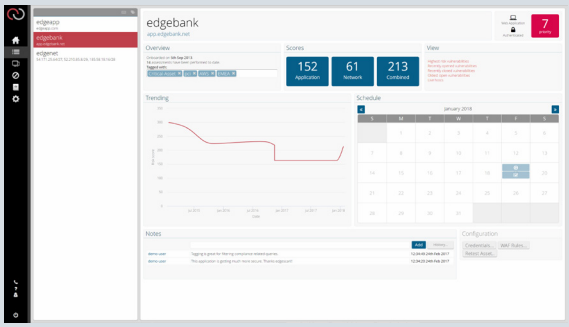
KNOWLEDGE

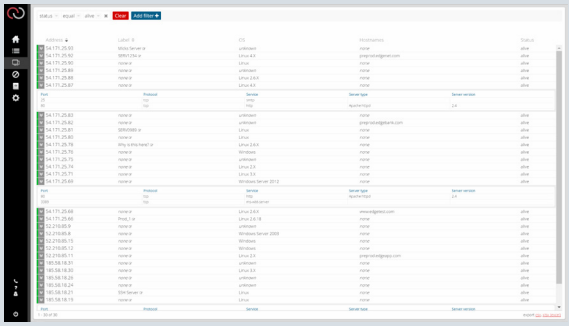
Developer training, frequent software assessment early in the development lifecycle and security analytics, are key to implementing a security program that compliments your organisations software development lifecycle.

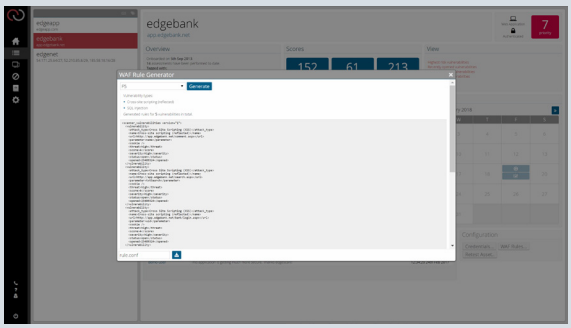
edgescan™ Portal











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.

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

Accuracy/Human Intelligance: All vulnerabilities discovered by edgescan™ are verified by our engineering team to help ensure they are a real risk and prioritised appropriately for our clients. Our analysts 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.

One-click WAF: Rule generation supporting a variety of firewalls is also supported, helping you virtually-patch discovered vulnerabilities.

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 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.

edgescan™ Gartner 2016 Tech Excellence Awards Winner PCI Approved Scanning Vendor CIO Review 20 Most Promising Enterprise Security Solution Providers - 2017 amazon web services Partner Network Technology Partner Contributor ISO 27001 Certification Europe

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