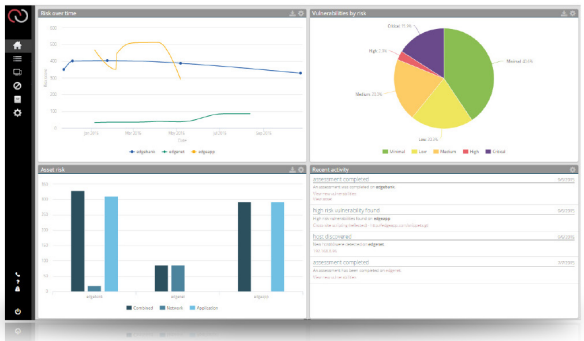
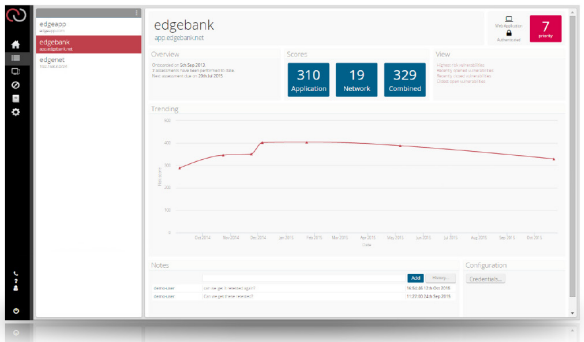
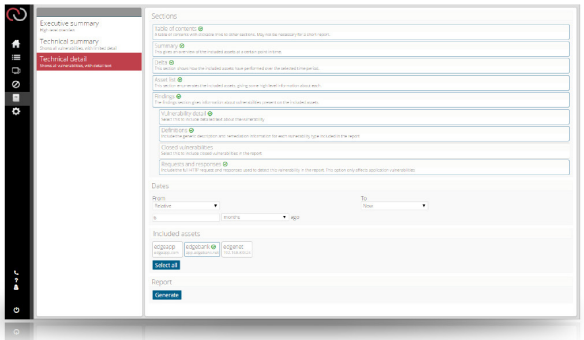
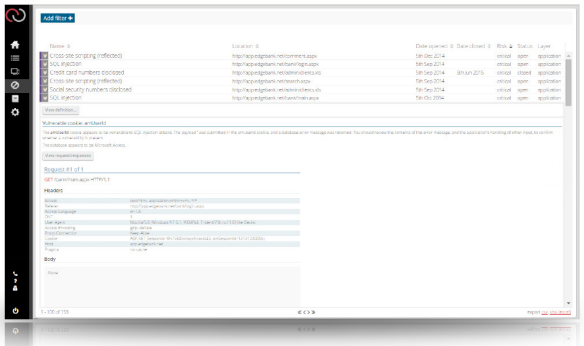
2016 Vulnerability Statistics Report

edgescan™ Portal









Introduction

Vulnerabilities or bugs in software may enable cyber criminals to exploit both Internet facing and internal systems. Fraud, financial, data & identity theft, and denial-of-service attacks are often the result, leaving companies with serious losses or damage to their reputation. However, some of these issues can be easily avoided or at least mitigated.

This document discusses the vulnerabilities discovered by **edgescan™** over the past year – 2016.

The vulnerabilities discovered are a result of providing "Fullstack" continuous vulnerability management to a wide range of client verticals; from Small Businesses to Global Enterprises, From Telecoms & Media companies to Software Development, Gaming, Energy and Medical organisations. The statistics are based on the continuous security assessment & management of over 57,000 systems distributed globally.

About edgescan™

SaaS: edgescan™ is a Software-as-a-Service (SaaS) vulnerability management service which helps detect vulnerabilities in both web application and hosting servers 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 systems technical stack.

Coverage: edgescan™ provides "full-stack" 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.

Accuracy/Human Intelligence: All vulnerabilities discovered by **edgescan™** are verified by our engineering team to help make sure they are a real risk and highlighted appropriately to our clients.

API: The API makes it very easy to plug edgescan into your ecosystem in order to correlate and reconcile, providing integration with both GRC and Bug Tracking Systems alike.

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

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

Scale: Managing estates from one web application to hundreds, from a single hosting environment to thousands, edgescan delivers continuous and on demand security assessments.

edgescan™

2016 Tech Excellence Awards Winner

Gartner

2016 in Review – Executive Summary

Many of the problems uncovered last year and the year before are still present. 2016 gave birth to IoT exploitation resulting in millions of "zombie" insecure devices being used for DdoS attacks. Large global organisations and governments were breached resulting in millions of client records being stolen.

Common vulnerabilities are still easy to find due to insecure programming practices. Cryptographic implementation flaws are still commonplace and patching of systems is still a large source of vulnerabilities.

How to improve security posture in 2017

Awareness, Detection and **Response** are key aspects in defending against cyber-attacks and **edgescan™** helps with this approach.

In terms of operational approaches, organisational trends towards DevSecOps should assist with security becoming more integrated and earlier in the system development lifecycle, "Pushing Left".

Hosting systems: Using Secure Baselines / Builds in cloud environments such that if vulnerabilities are discovered rather than patch, a new baseline is deployed. - one approach we see being more commonly used.

Error monitoring and log analysis solutions are also assisting with detective controls and helping organisations detect anomalies earlier and reacting quicker.

Overall host/server security below layer 7 is still a rich area for vulnerabilities.

Application Layer: A drive towards DAST and SAST integration into the build process is catching issues "early and often" which assists in more secure software.

We still see "component security" being overlooked. Components are defined as open source code, frameworks and code used by developers but not written by the application developer teams.

Patching and component management relates to both web application and hosting servers both running insecure instances and services. In terms of web applications many instances of insecure frameworks, plugins and components to support Cryptography, HTTP, language processors and parsers, contained exploitable vulnerabilities.

In addition the operating systems and services supporting such components also had vulnerabilities.

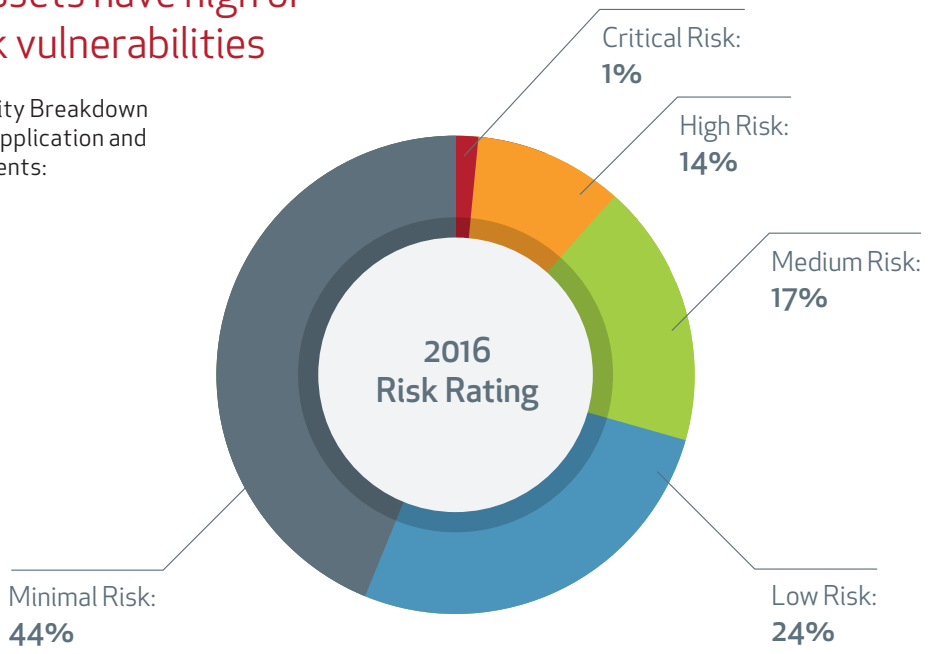
Our measuring tool and data repository

The vulnerability data used for this report is the result of what was discovered on our clients systems over the past calendar year (2016). All of the findings in edgescan are manually validated and risk rated to ensure accuracy and also to assist our clients in understanding which issues need to be prioritised.

Assets: edgescan™ assesses both server and web application layer systems for vulnerabilities (Fullstack). For our clients we call these collectively "Assets". This gives our clients the ability to group similar and related systems into asset groups for easier management and to aid alignment to organisational structure.

15.1% of Assets have high or critical risk vulnerabilities

Overall vulnerability Breakdown across both web application and hosting environments:



High or critical vulnerabilities are defined as:

- Easily exploitable
- Usually remote from the public Internet
- Application and Network layers combined
- Root Cause: Coding errors, configuration flaws and out-of-date or no patching applied

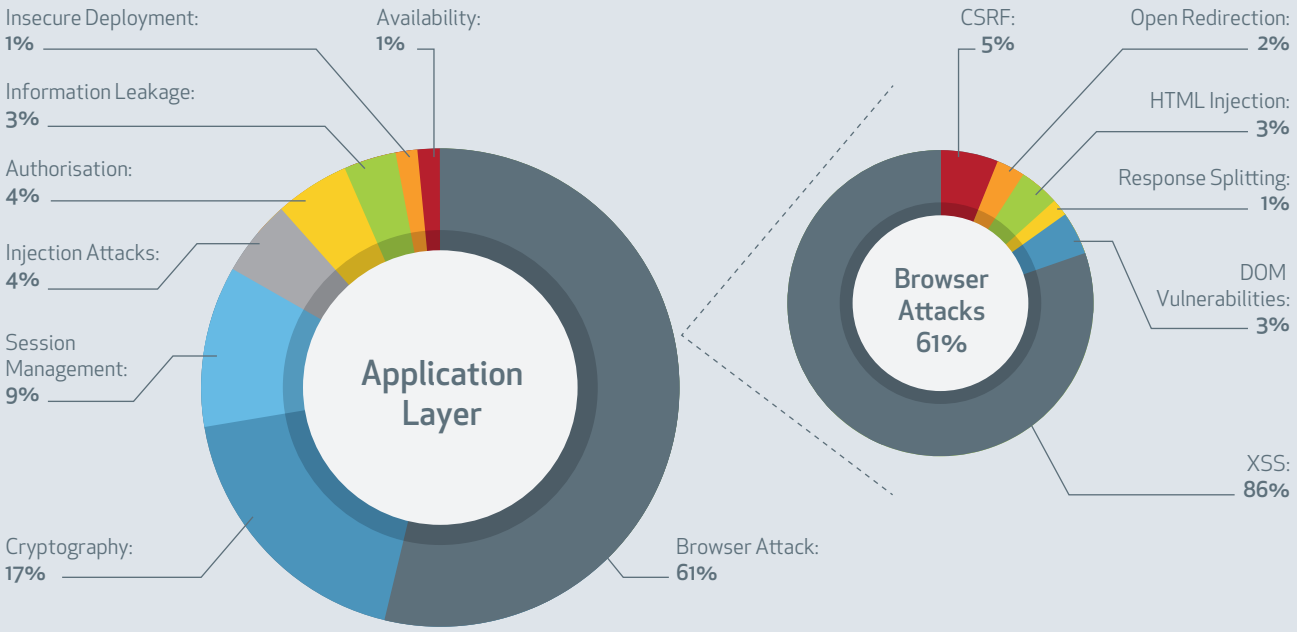
Remediation: Even though patch management is less than glamourous it still needs to be consistently performed. Security patches are a result of security bugs being discovered in application component and server systems provided by third parties.

In relation to web application security we still talk about Secure Application Development. It's our view that security touch points and developer education is a good starting place to correct the problem.

Vulnerability Statistics

Web Applications and Web Site Security

Likelihood of a vulnerability being discovered – Web Applications



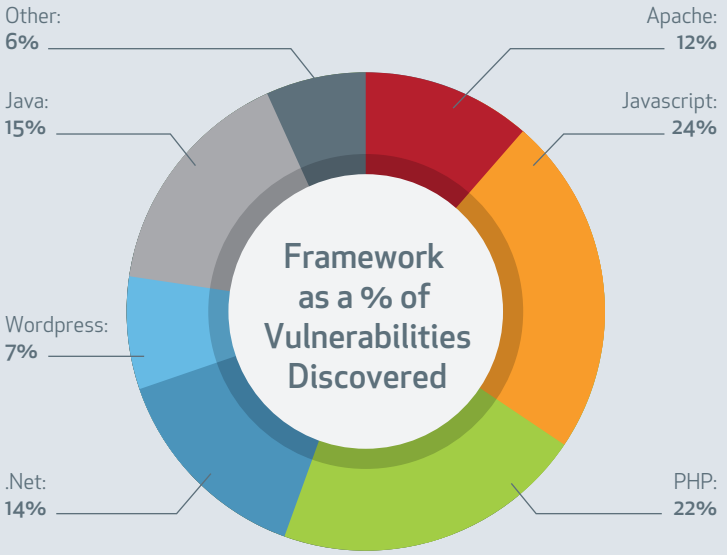
Above is a snapshot of the most common vulnerabilities in 2016 for in the web application layer as discovered by **edgescan™**. As you can see the majority of issues are related to "browser attacks" and weaknesses in cryptography. SQL Injection is thankfully less common, akin to other injection (Command Injection, Remote Code Execution vulnerabilities), all of which can result in total system-wide compromise.

Likelihood of a vulnerability being discovered by framework or language

Javascript and PHP vulnerabilities were found to result in a large proportion of security weaknesses. Not forgetting Java based technologies and frameworks, many of the vulnerabilities discovered were a result of poor component or framework patching.

"Apache based technology (Tomcat, Apache Server, HTTP Server, Mod_*) is a common source of vulnerabilities due to poor configuration and poor patching policies.

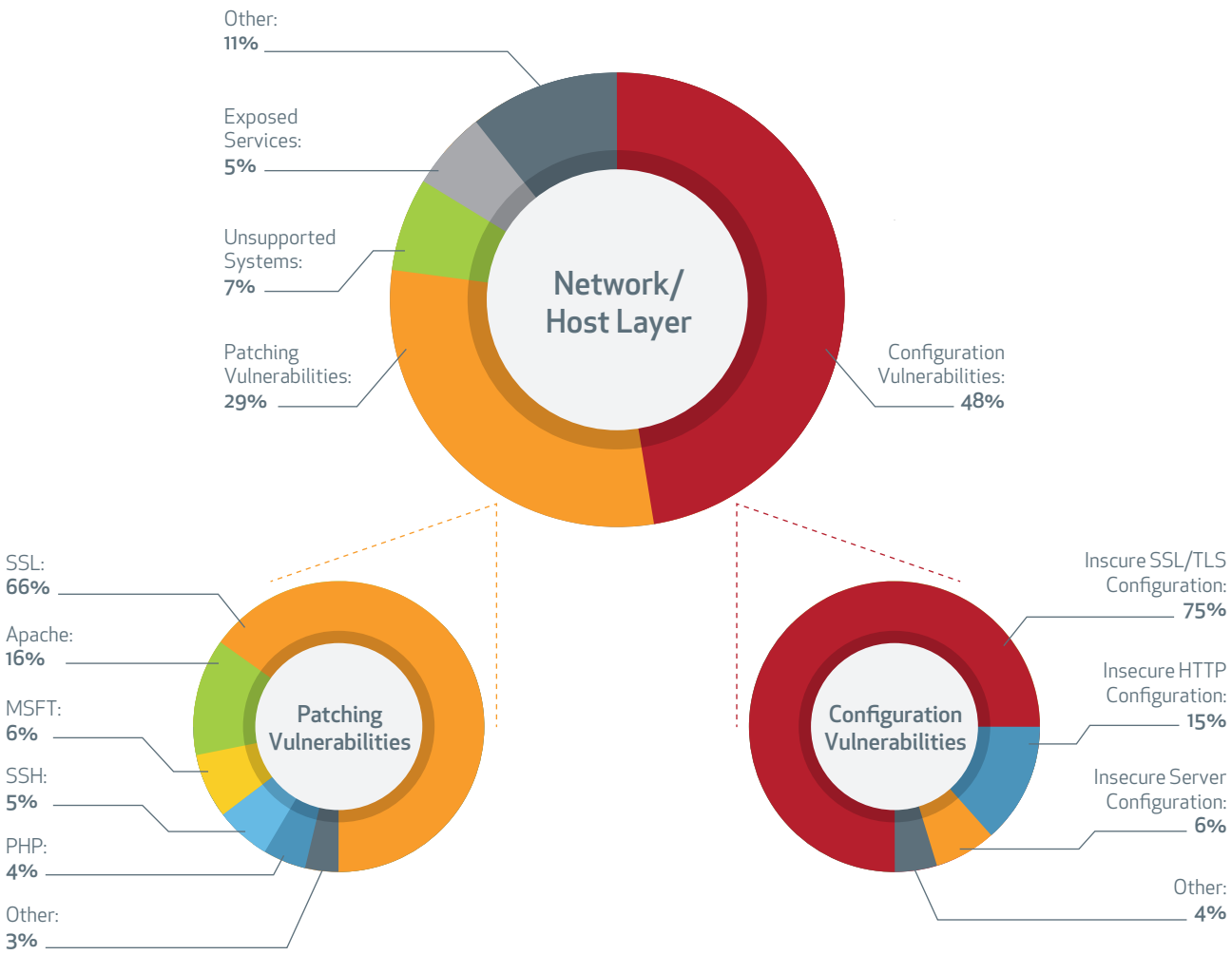
Javascript and PHP coding errors and deprecated packages such as Jquery are also a source of vulnerability."



Hosting Layer Vulnerabilities

What types of hosting & deployment weaknesses are common?

A large percentage of vulnerabilities in the hosting layer were as a result of either poor patching or poor configuration - 77% combined.



In particular, encryption technologies (SSL/TLS) were the root cause of a high percentage of both configuration and patching issues, 75% and 66% respectively. The high occurrence of SSL weakness is a legacy problem given that SSL has been found out to be flawed (see Poodle/Heartbleed) and it is recommended to move to TLS 1.2 if possible.

Heartbleed: http://heartbleed.com

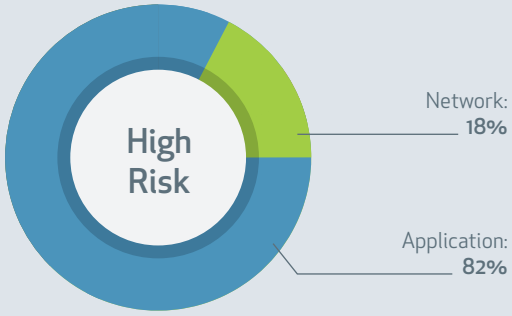
Shellshock: https://en.wikipedia.org/wiki/Shellshock_%28software_bug%29

LogJam: https://en.wikipedia.org/wiki/Logjam_(computer_security)

Vulnerability Dispersion

Where do the vulnerabilities live?

In 2016 we discovered on average 35% of all discovered vulnerabilities were associated with web applications and 65% deemed hosting layer weaknesses.



What is interesting about this finding is that the majority of high and critical risks are associated with web applications even though the majority of vulnerabilities discovered were hosting layer issues!

How is risk dispersed across the stack?

- 95% of Critical risks were discovered in the web application layer
- 5% of Critical risks were in Network Layer
- 82% of High risks were discovered in web application layer
- 18% of High Risks were in the Network Layer

95% of the critical risks discovered across the "Fullstack" can be attributed to the web application layer. 18% of high risk vulnerabilities can be attributed to the Hosting/ Network Layer.

Time-2-Fix

How fast are we fixing vulnerabilities?

In terms of vulnerability mitigation the turnaround time varies depending on where in the stack the discovered vulnerability resides.

It appears patching of systems for known vulnerabilities (CVE's) can be achieved in a relatively short amount of time.

Time-To-Fix has security significance when looking at the size of the Window of Exposure for a given system.

Code: Time-To-Fix for code level (developer bugs) vulnerabilities can be fast particularly in the case of new deployments. Older web deployments appear to take more time to remediate mainly due to lack of knowledge of the code-base or the web application not being on the current critical path for the business in terms of assignment of resources to address the issue.

Patching: Time-To-Fix for patching appears to have the fastest turnaround time. This is due to the apparent and relative ease of applying patches to operating systems and services.

Average Time to fix

(Network and Application layers combined)

- Critical: 50 days
- High: 59 days
- Medium: 72 days

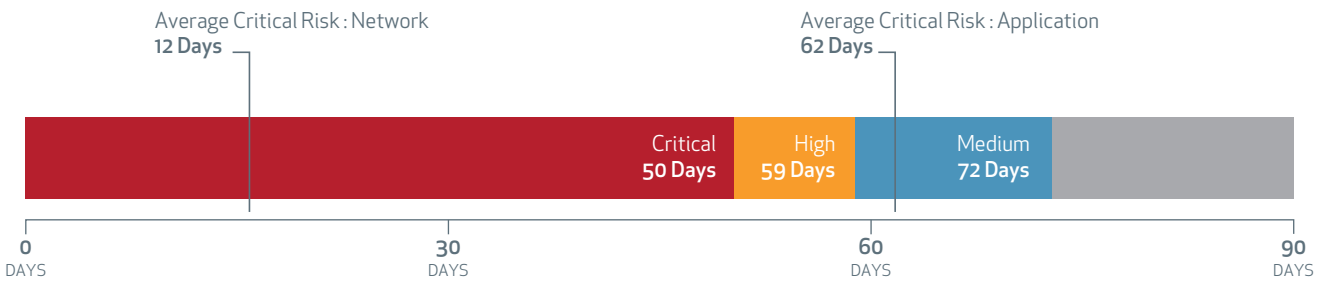
Average Time to Fix (Application)

- Critical: 62 days

Average Time to Fix (Network)

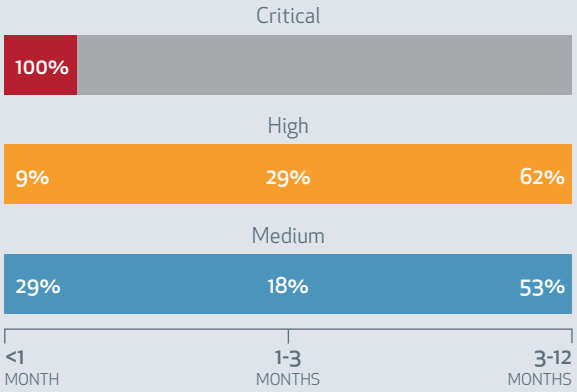
- Critical: 12 days

AverageTime to Fix

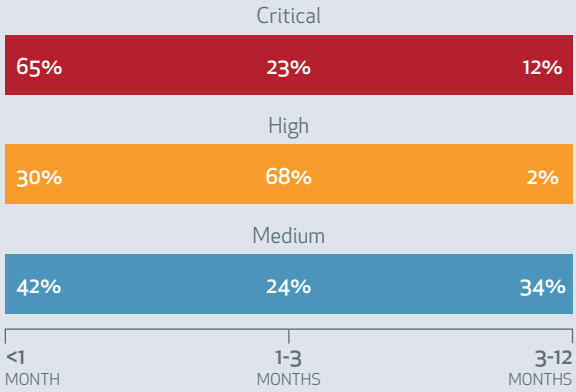


"Web Application vulnerabilities take longer to fix. They are also more likely to be of higher risk (95% of critical risk issues are in the web layer). Continuous assessment and preventative activities such as SDLC security can assist in reducing risk density and lower time-2-fix"

Time to Fix (Network)



Time to Fix (Application)



Network Layer:

- 100% of Critical Vulnerabilities appeared to be fixed within 1 month
- 9% of High Risk Vulnerabilities appeared to be fixed within 1 month
- 29% of Medium Risk appeared to be fixed within 1 month
- 63% of High Risk Vulnerabilities were fixed between 3-12 months
- 53% of Medium Risk Vulnerabilities were fixed between 3-12 months
- 0% Critical Vulnerabilities aged more than 1 month
- Oldest Network Vulnerability: 258 days old

Application Layer:

- 65% of Critical Vulnerabilities appeared to be fixed within 1 month
- 30% of High Risk Vulnerabilities appeared to be fixed within 1 month
- 42% of Medium Risk appeared to be fixed within 1 month
- 12% of critical risks took from 3-12 months to fix
- 3% of high Risk Vulnerabilities took 3-12 months to fix
- Oldest Application Vulnerabilty: 324 days old

Oldest Critical Vulnerabilities

Time 'the fire in which we all burn'.

Some vulnerabilities in edgescan™ which have taken a prolonged period of time to fix or mitigate.

Oldest "Known" vulnerability discovered in 2016 by edgescan™:

CVE-2007-6420 - Cross-site request forgery (CSRF)

CVE-2007-3847 - Apache 2.3.0 DoS

CVE-2007-5000 - Apache HTTP Server XSS

CVE-2007-6388 - Apache HTTP Server XSS

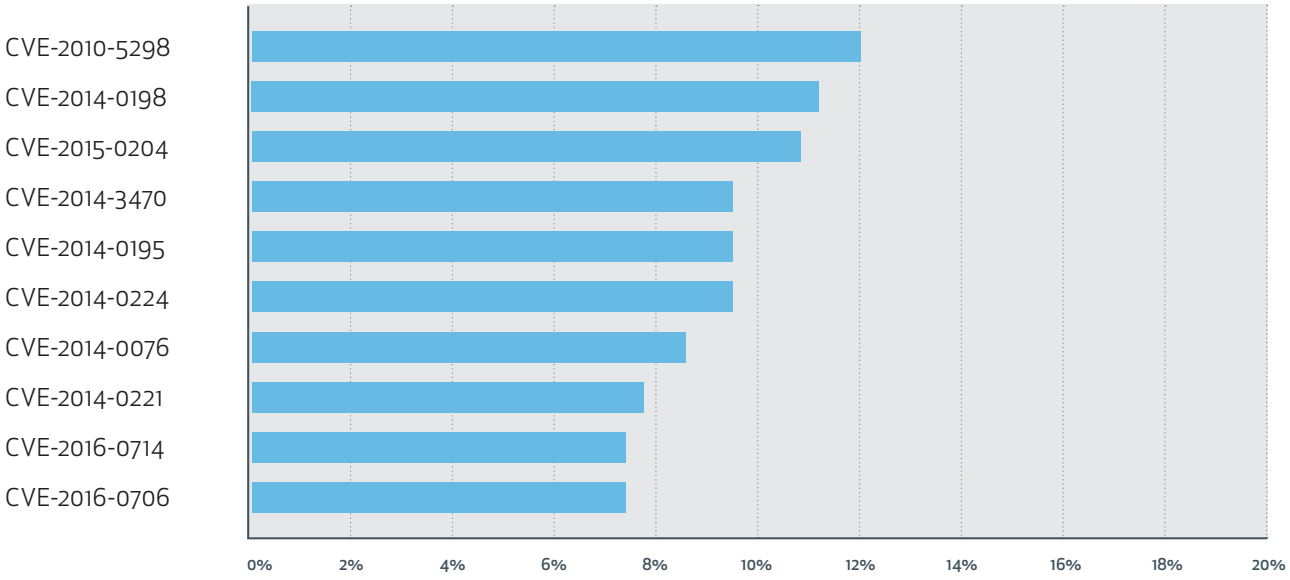
9 year old vulnerabilities exist in the wild on live servers. Poor or non-existent patching is a major root cause, downloading frameworks with known vulnerabilities out-of-the-box is also a root cause – component version management.

The good news is that the frequency of occurrence is between 1.5% and 3%

"Known" Vulnerability Frequency

Regarding known vulnerabilities, CVE's, the most common vulnerability is as follows:

Most Common Know Vulnerabilities



Note the 6-year-old CVE-2010-5298 with the likelihood of occurring of 12%.

Simple activities such as patching, system inventory and system maintenance are still lacking. A consistent approach to patching and system maintenance can reduce the attack surface significantly.

What is edgescan™?

edgescan™ is a managed security service which identifies and provides vulnerability intelligence on an on-going basis. It detects technical vulnerabilities in both internal and Internet facing systems and provides you with the power to understand, prioritise and fix.

It provides you the ability to manage both network and web application security issues for tens, hundreds or even thousands of your systems.

edgescan™ conducts Application & Server vulnerability management with manual validation to help ensure your application / server security.

edgescan™ reports are virtually False Positive free due to our hybrid approach of combining automated testing with manual validation.

edgescan™ provides continuous asset profiling letting you see what systems and services are live and available at any point in time and provides alerting to let you detect rogue, APT or delinquent systems within your asset estate.

edgescan™ gives you:

- Unbeatable price-performance ratio
- Continuous Asset profiling and Alerting
- Continuous vulnerability assessment across both web and hosting layers
- Manual threat verification and accuracy of all issues reported - false positive free
- Prioritisation of security risks and remediation advise from our experts
- 24/7 dashboard access and customisable reporting
- Integration via API to GRC/ Bugtracking/JIRA/Slack & Automatic WAF Rule integration

edgescan™
DIGITAL SECURITY RADAR

False Positive Free, Full-Stack, Continuous Penetration Testing.

"Very useful and helpful – helped us find a lot of issues quickly and very cost effective for the benefit delivered for us."

CISO Financial Services, UK

"Great customer focused service, and the clear explanation of the results from pen tests has certainly made our life easier."

IT Architect, Legal Firm, UK&I

"Excellent service, quick response, efficient and unobtrusive. Highly recommended."

CISO Media Organisation, USA

"Apart from a strong technical platform, the key advantage Edgescan seems to have over competitors is an ability to relate knowledge of the subject matter to real world actions..."

Head of Application Security (Medical Organisation), Dublin, Ireland

"...very successful service for us and has provided a focus to our teams to ensure we are constantly improving our security posture. Most importantly, being regular, it's no longer just a once a year focus."

Gaming Client, EU

2016 Tech Excellence Awards Winner

Gartner

edgescan™
www.edgescan.com

© 2016. BCC Risk Advisory Ltd. www.bccriskadvisory.com

edgescan™

CONTINUOUS VULNERABILITY MANAGEMENT

Email: info@edgescan.com Telephone: +353 (1) 681 5330
www.edgescan.com