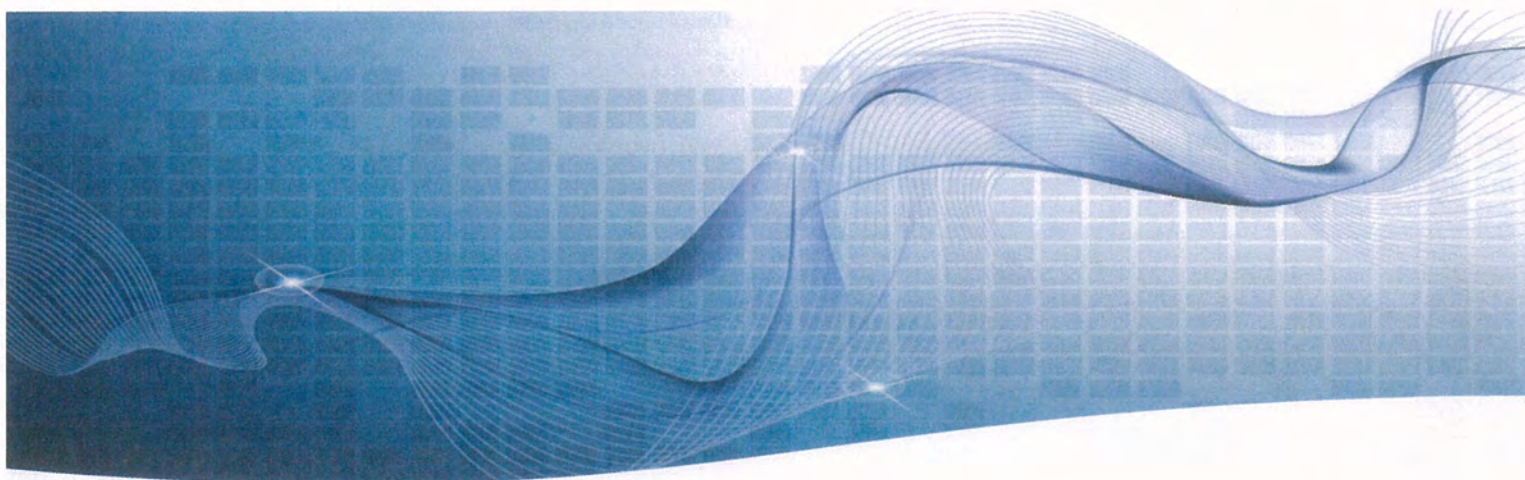




Report

ENTERPRISE SECURITY ENTERPRISE SOLUTIONS

City of Joondalup Social Engineering - Phishing



■ Published: 18/06/2018

■ ES2 Ref: 18-WA-CoJ-SE-6

■ **Perth Business Centre**
Level 27,
44 St. George's Tce.
Perth WA 6000

■ **Perth Operations Centre**
"The Factory"
69 King St.
Perth WA 6000

■ **Brisbane**
Suite 18, Level 10
320 Adelaide St.
Brisbane QLD 4000

■ **Sydney**
Level 12,
95 Pitt St.
Sydney NSW 2000

■ **Paris**
4 rue Neuve de la
Chardonnière
75018 Paris,
FRANCE

Document Information

Author/Custodianship

Author:	Cordelia Mortimer-Lee
Custodian:	ES2
Type:	Report

Document Version History

Version	Date	Change By	Amendment
0.1	15/06/2018	C Mortimer-Lee	Original Draft Version
0.2	15/06/2018	C Wright	QA Review
1.0	18/06/2018	S Simpson	Released for Publication

Project Information

Client:	City Of Joondalup	ES2 PM:	Christie Wright
Project Name:	Social Engineering - Phishing	ES2 Stream:	Enterprise Security
Client Contact:	Greg Burgess	Prepared By:	Cordelia Mortimer-Lee
ES2 Ref:	18-WA-CoJ-SE-6	Date Produced:	18/06/2018

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.

ES2 - City Of Joondalup - Social Engineering - Phishing – Report ■ Ref: 18-WA-CoJ-SE-6

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Table of Contents

1. Executive Summary	5
2. Introduction	7
3. Email-based Phishing Campaign	8
3.1. Target Acquisition	8
3.2. Hook and Infrastructure Generation	8
3.3. Attack Delivery	10
3.4. Results	10
4. Risk Assessment Matrix	11
5. Next Steps	14
Appendix A: Definition of Terms and Acronyms	15

List of Figures

Figure 1 – Summary of Findings	5
Figure 2 – City Of Joondalup Results Summary	6
Figure 3 – Social Engineering Phishing Approach.....	8
Figure 4 – Example Phishing Email.....	8
Figure 5 – Initial Phishing Landing Page.....	9
Figure 6 – City Of Joondalup Interaction Results.....	10

1. Executive Summary

ES2 were engaged by the City of Joondalup (CoJ) to perform a social engineering campaign to assess the risk of exposure to common social engineering techniques. A phishing campaign was delivered at the request of the City of Joondalup technical contact, Greg Burgess.

At the request of CoJ, a 'Black Box' testing approach was taken to source target information, this term refers to an engagement where the assessor has no prior information of the internal CoJ system or staff. Instead the ES2 assessor gathered information using only publicly available sources. This allows the assessment to be representative of a genuine attack and test CoJ's in place anti-phishing systems.

A frequently overlooked factor in information security is the threat from Social Engineering, "the use of deception to manipulate individuals into divulging sensitive or personal information that may be used for fraudulent purposes." This report details ES2's findings, which highlights how the successful exploitation of common social engineering techniques, resulted in the ES2 assessor gaining access to sensitive information. These details were specifically staff log-on credentials, which vastly increased the potential of a deeper penetration of the CoJ infrastructure.

There was a small number of individuals who demonstrated a reasonable level of security awareness, who alerted internal IT administration on receipt of a suspicious email during the phishing engagement. However, staff appeared to have discussed amongst themselves the presence of the phishing email and by the third day the entire office was aware of the campaign.

Overall, the engagement has identified 3 findings that have been documented across the campaign. This rates CoJ with an overall organisational risk posture of "Medium", this directly relates to the large amount of interaction between staff members and the phishing email.

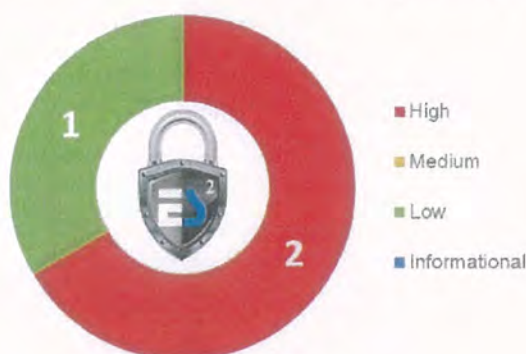


Figure 1 – Summary of Findings



Campaign Summary

A total of 100 employees contact details were identified using Open Source Intelligence Gathering (OSint) techniques and 98 emails were sent in total. Of the 98 emails sent, 79 user accounts were identified as successfully receiving the phishing email, 47% (37) of CoJ users opened the email, a further 21% (17) clicked the link and 18% (14) entered what is believed to be, their login credentials.

It must be noted that in a real-world situation it only takes a single susceptible user to enable a successful attack against an organisation.

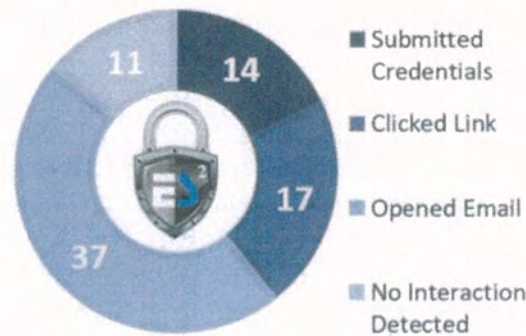


Figure 2 – City of Joondalup Results Summary

On a positive note, of the 79 users who received the emails, several users contacted the IT department reporting the receipt of possible spam. It was also reported that, while no further staff approached IT, word of mouth throughout the organisation quickly spread that the email was a phishing email and user interaction significantly dropped off. This suggests evidence of a security-conscious environment within CoJ.

2. Introduction

ES2 were engaged by CoJ to conduct a social engineering assessment in order to identify the current state of its employees' security awareness. This also enables CoJ to gain a sense of the general susceptibility and likelihood of success from such an approach by genuine attackers.

Discussions with the CoJ's technical contact were undertaken to establish and approve the social engineering techniques used in this engagement to ensure that they met the ethical and moral standards of CoJ.

Social Engineering tests carried out were restricted to the following during this engagement:



Phishing

The use of email in an attempt to lure a user to perform an action that will allow an unauthorised person access to information or resources not intended for public consumption.

3. Email-based Phishing Campaign

The email-based Phishing campaign was segmented into four major components: Target Acquisition, Hook and Infrastructure generation, Attack delivery and Reporting:

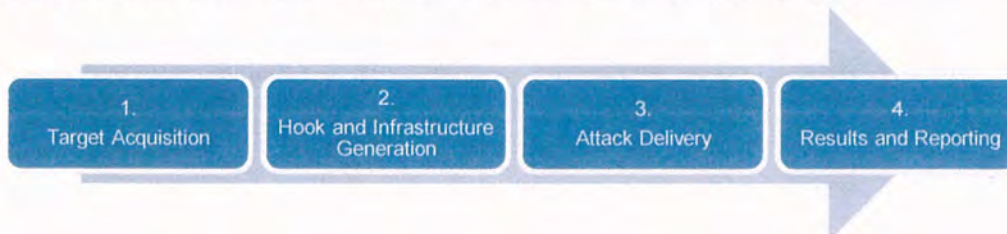


Figure 3 – Social Engineering Phishing Approach

3.1. Target Acquisition

The details of 100 CoJ users were identified by the assessor through Open Source Intelligence Gathering (OSInt). These 100 targets were then sent to the technical contact for confirmation and were subsequently approved as being the target list. These users represented a cross-section of all employees of CoJ at various levels and with various roles.

3.2. Hook and Infrastructure Generation

The overall scenario, the phishing email, the target web page and related infrastructure were all developed by ES2 and was then approved by the CoJ technical contact. The scenario involved sending an email from 'helpdesk@wagov.info' to the identified targets, this email/web domain was purchased by the assessor for a minimal amount specifically for this engagement. The email asked them to follow the link embedded within the email and fill out a short security survey to assist in improving the organisation's security levels. Upon clicking the link within the email, users were taken to an ES2 crafted web login page to access the survey, this page had the look and feel of the genuine CoJ login page.

Dear {{.FirstName}},

As part of the City of Joondalup's ongoing commitment to security, it is requested that all staff complete the [following short survey](#) within 72 hours.

The survey contains 21 quick questions, and should take 15 minutes at most to complete. The results will be returned to City of Joondalup anonymously. The survey is designed to give an accurate representation of current staff security awareness, and your input will help to ensure the confidential material of the City of Joondalup is kept secure.

Additionally, completing the survey within 72 hours will enter you in the draw to win one of three \$200 David Jones gift card! Winners will be announced Friday the 15th of June at 4pm.



[Take Survey](#)

IT Services

Email: helpdesk@wagov.info

Phone: 9400 4000

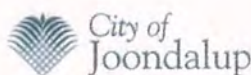


Figure 4 – The Phishing Email

In addition to enticing users to follow the initial phishing link, an effort was made to extract their login credentials. Given this, an SSL certificate was generated in relation to the purchased domain to firstly, add face legitimacy to the phishing attack but more importantly, to protect any potential CoJ credentials during transit.

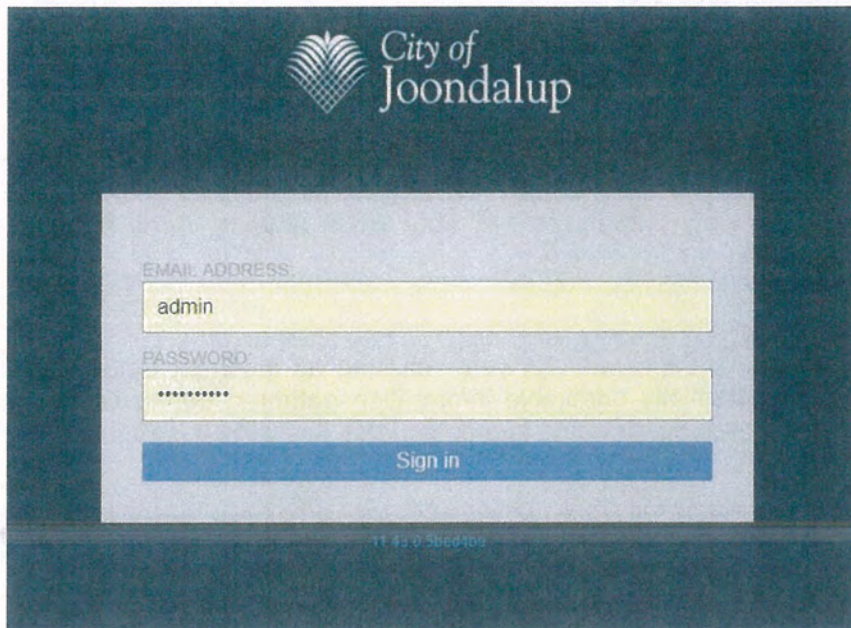


Figure 5 – Initial Phishing Landing Page

Each targeted email address was assigned a unique identifying code, as a means of associating any response to specific users. This provided traceability and metrics for reporting purposes, as well as preventing the incorrect duplication of findings (for example, if the same user followed a link twice).

3.3. Attack Delivery

The attack was launched at approximately 8.30am on 12th June 2018. The release of the phishing emails were staggered, approximately 15 emails were delivered every 5 minutes to the CoJ targets. This approach can help to avoid potential spam or security filters, which may otherwise delay or inhibit the delivery of the campaign.

In all, a total of 98 emails were sent to CoJ targets. 19 accounts returned an undeliverable response, resulting in 79 successfully delivered emails. This undeliverable response is likely due to the details be outdated and possibly associated with persons no longer employed by CoJ.

Following the delivery, the ES2 controlled hosting infrastructure was monitored for user engagement, this included the potential submittal of login credentials by the targets. This monitoring process continued until approximately 5.00pm on 14th May 2018, allowing three business days for user responses to be recorded.

3.4. Results

Of the 98 emails originally deployed, 19 were returned as incorrect email addresses, which is expected when using potentially unreliable information gathered during OSInt. No emails were returned with any automated out of office responses, this suggests it is possible that CoJ does not require staff to use them.

Of the 79 CoJ user accounts identified as successfully receiving the phishing email, 37 were detected to open the email, of which 17 engaged with or clicked the embedded HTML link. 14 of these targets interacted further with the spoofed website by submitting their credentials.

Of the 14 users who submitted their credentials, 12 then continued to complete the security questionnaire.



Figure 6 – City of Joondalup Interaction Results

On a positive note, several targets confirmed to have received the email and flagged their suspicions to the internal CoJ IT team. Furthermore, whilst IT were instructed not to issue an alert to the spoof email, staff are reported to have alerted each other to the suspicious email of their own accord through word of mouth. This response suggests a positive security culture has been encouraged within CoJ and should be commended.

4. Risk Assessment Matrix

The chart below has been developed to assist organisations in understanding the identified risks. Findings are ranked in the following categories; High, Medium, Low and Informational. Included is a brief description of the type of vulnerability, an explanation of the risk and the recommendations for mitigation, or otherwise reducing the risk to the organisation.

Risk Assessment Matrix	
High	High findings are those that have the potential to lead to an unauthorised person gaining access to: • Personal information of a large number (>50%) of staff details; • Unsupervised access to sensitive working areas; • IT systems access to the extent that they can add a user (or administrator) account to a network; • Gain network access (local or remote) for an unauthorised device; • Access to existing user's login credentials; • Access to information that is considered by the business to be sensitive (i.e. board papers, financial details).
Medium	Medium findings are those that have the potential to lead to an unauthorised person gaining: • Access to personal information of a large number (10% - 50%) of staff details; • Unsupervised access to working areas; • Control over IT systems to the extent that they can: ○ Add a local user; ○ Exfiltrate or infiltrate documents via USB; ○ Physically connect an authorised device.
Low	Low findings are those that have the potential to lead to an unauthorised person gaining: • Access to personal information of a number (<10%) of staff details; • Knowledge of internal systems or "lingo" that can aid a user in developing an attack.
Informational	Informational findings are those where the vulnerability or weakness that did not directly result in any form of unauthorised access but is worthy of noting for future reference.

H01	Phishing Target Engagement	Prioritisation:	HIGH
Description			
User engagement was identified across different targets, this engagement included the clicking of the fraudulent link and the submitting of potential login credentials. Some of the targets who input their credentials were in roles granting them access to privileged functions and potentially sensitive information.			
Risk			
The use of phishing methodologies is an extremely common technique deployed by real-world attackers (social engineers). A lack of user awareness significantly increases the likelihood of a phishing email being followed and engaged with. This in turn increases the likelihood of successful account and/or network compromise. The input of system administration credentials is particularly concerning, as access to this account has the potential to grant access to large amounts of information of other staff members as well as allowing the user considerable privilege to system and network functionality. Any interaction with a phishing email (such as loading of external content, clicking a link or replying to the email itself) will reveal information to an attacker. This includes information seemingly innocuous information such as current browsers and browser versions, internal IP addresses and hostnames, external IP addresses and personal details such as; additional email addresses, contact numbers or email footer styles.			
Recommendation			
Develop/update and carry out a program of security awareness training to communicate with users the up to date threats associated with social engineering and phishing attacks. This must include how to identify potentially malicious emails and how users should react if they suspect they have received one. Prescribed reactions should include reporting the email and avoidance of further interaction with the email or sender.			

H02	Weak Password Identified	Prioritisation:	HIGH
Description			
Numerous passwords were identified that would be considered weak in security terms, including passwords that contained information specific to the user such as; their own and children's names or simple dictionary words with minimal numbers attached.			
Risk			
The function of passwords is to authenticate users, therefore weak passwords can increase the likelihood of successful attacks against user accounts. This can lead to system and network access by an attacker, which can lead further lead to access to sensitive resources. This finding was inferred from user-submitted passwords, and as such, contains a low possibility of being a false positive finding.			
Recommendation			
Enforce the use of strong passwords on impacted accounts. Privileged accounts (such as Administrators) and those with privileged access rights (such as Remote Desktop or remote access) need to be prioritised. It is highly recommended that a program of security awareness training for staff should include emphasis on the selection of strong passwords. This should include; references to the risks of password reuse across different services, avoidance of common passwords, dictionary words and words related to the user or organisation and avoidance of repetition.			

L01	External Resource Loaded	Prioritisation:	LOW
	Description		
	A tracking image embedded within a phishing email was loaded. This suggests that either the users email system/program was configured to automatically load external content, or that the user consciously accepted warning notifications regarding the risk of loading such content.		
	Risk		
	The loading of external content in general, including tracking images, can be used to trace user activities. For example, determining when an email is accessed or opened. In addition, as the request is made by the client, it can reveal basic information about the environment such as; external IP addresses, browser types and operating system versions in use. In this case, the risk associated with this finding were slightly lower, given the technical security controls in place by CoJ.		
	Recommendation		
	Configure email clients to disable the automated loading of third party images and content. In addition, training should be given to users on the implication or potential security risks of allowing such content.		

5. Next Steps

ES2 recommend that CoJ conduct a series of security awareness training sessions in order to raise awareness of Social Engineering within the work place.

ES2 also recommend that a repeat social engineering assessment be conducted approximately three to six months after delivery of the security awareness education sections to measure effectiveness of the education.

The best practice for information security is to provide security awareness training on induction and then on-going refresher training conducted annually at a minimum. Ad-hoc security warnings should also be provided from a known IT contact point when required.

Topics recommended for inclusion within the awareness training program include, but are not limited to:

- Security within email use, including:
 - General awareness of suspicious communications;
 - Verification of email sender; and
 - Checking of links.
- Threats from other communication vectors (SMS, chat etc.);
- Awareness of social engineering techniques.

This report should serve as a valuable baseline of CoJ's current resilience to Social Engineering threats. This can only be improved upon and continue to foster a cyber-security-aware culture.

Appendix A: Definition of Terms and Acronyms

The following terms and acronyms have been used within this report:

Table 1 – Terms and Definitions

Term/Abbreviation	Meaning
Phish/Phishing	A form of Social Engineering attack utilising email as the delivery mechanism.
Pretext	A story or "lie" designed to exploit a person's trust or psyche.
Spoof	A term used by hackers for a hoax or duplicate of an original.
URL	Uniform Resource Locator eg: www.google.com.au
Vulnerability	A gap in security that has the potential for exploit.

End



ENTERPRISE SECURITY ENTERPRISE SOLUTIONS

ATTACHMENT 2

Report



City of Joondalup External Penetration Test

■ Published: 19/07/2018
■ ES2 Ref: 18-WA-COJ-SE-6

■ Perth Business
Centre
Level 27,
Tce.
Perth WA 6000

■ Perth Operations
Centre
69 King St.
Perth WA 6000

■ Brisbane
Level 18,
123 Eagle St.
Brisbane QLD 4000

■ Sydney
Level 12,
95 Pitt St.
Sydney NSW 2000

■ Paris
4 rue Neuve de la
Chardonnière
75018 Paris,
FRANCE

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Document Information

Author/Custodianship

Author:	Michael Ransom
Custodian:	Steve Simpson
Type:	Report

Document Version History

Version	Date	Change By	Amendment
0.1	12/07/2018	M. Ransom	Original Draft Version
0.2	16/07/2018	C. Wright	QA Review
0.3	18/07/2018	S. Simpson	Authorised for release

Project Information

Client:	City of Joondalup	ES2 PM:	Christie Wright
Project Name:	External Penetration Test	ES2 Stream:	Security
Client Contact:	Greg Burgess	Prepared By:	Michael Ransom
ES2 Ref	18-WA-COJ-SE-6	Date Produced:	19/07/2018

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 2 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Table of Contents

Document Information.....	2
Author/Custodianship	2
Document Version History	2
Project Information	2
1. Executive Summary	5
2. Approach.....	6
2.1. Methodology	6
2.2. Planning	6
2.3. Discovery	6
Application	7
2.4. Attack	10
webmail.joondalup.wa.gov.au	10
Check Point VPN	11
Cisco Smart Install	11
events.joondalup.wa.gov.au	11
www.joondalup.wa.gov.au and m.joondalup.wa.gov.au.....	12
Flash Cross Domain	12
3. Results and Findings	13
3.1. Results Overview	14
3.2. Detailed Technical Results	16
4. Next Steps	24
Definition of Terms and Acronyms	25

List of Figures

Figure 1 - Risk Summary	5
Figure 2 – NIST based Methodology.....	6
Figure 3 - Check Point Connection	11
Figure 4 - WordPress Session	12
Figure 5 - WordPress Admin Console Filtering	12
Figure 6 - Severity Scale.....	13

List of Tables

Table 1 – Service Discovery	7
Table 2 – City of Joondalup Confirmed Credentials	10

1. Executive Summary

As part of a proactive security assessment, ES2 were engaged by City of Joondalup (CoJ) to perform a penetration test against their externally-accessible infrastructure.

The main point of contact for the City of Joondalup was Greg Burgess, Network Services Coordinator, who provided all necessary information required for testing.

Five (5) high risk vulnerabilities were discovered during testing. These risks primarily relate to weak passwords, outdated applications and overly permissive policies. There were some positive signs during testing, the defensive mechanisms City of Joondalup had in place reduced the overall vulnerability count. Additionally, one of the high-risk findings was resolved by the CoJ IT team prior to the conclusion of the test and as a result has not been included in the final risk summary below.

In all, a total of 14 vulnerabilities remained at the end of the test.

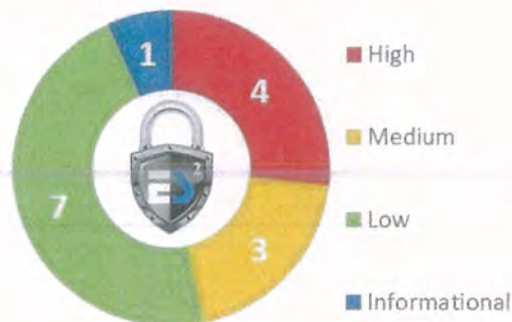


Figure 1 - Risk Summary

Overall, it is assessed that the City of Joondalup's external facing infrastructure represents a **medium to high** risk to the business operations of City of Joondalup.



To limit the risks associated with the vulnerabilities discovered, it is recommended that City of Joondalup implement the remediation actions suggested within this report. These include, but are not limited to:

- Adjust configuration surrounding certain security controls and accounts;
- Educate users on the importance of secure password selection;
- Update applications and components; and,
- Adjust encryption usage and algorithms.

If City of Joondalup can address these risks, they will greatly decrease their overall threat surface, consequently reducing the chance of a successful network penetration.

2. Approach

2.1. Methodology

The penetration testing assessment was carried out as a four-step process, based primarily on the NIST methodology, sourced from NIST 800-115. The US National Institute of Standards and Technology (NIST) have been responsible for the generation of many globally respected information security standards and guidelines, with their high-level penetration testing methodology outlined below:



Figure 2 – NIST based Methodology

All border gateway testing was conducted from locations external to City of Joondalup, to accurately simulate an attack from an Internet-based perpetrator.

Due to the nature of penetration testing ES2 cannot guarantee that all vulnerabilities have been discovered or documented. This penetration test was conducted utilising industry standards. Due to the ever-changing nature of online threats the findings of this report will become less valid over time.

2.2. Planning

The scope of work for this engagement consisted of assessing the potential vulnerabilities that exist within City of Joondalup external penetration test. The associated endpoints were identified as being positioned at the following IP address ranges:

- 203.161.120.65-203.161.120.126
- 103.233.148.10
- 103.233.148.130

The assessment activities consisted of:

- Scanning and enumeration of services currently operating within the scope;
- Determination of possible vulnerabilities identified within services discovered;
- Assessment and attempted exploitation of vulnerabilities, to eliminate false positive indications and penetrate the scoped network as much as possible; and
- Reporting of any identified penetrations, vulnerabilities, and recommended remediation advice.

2.3. Discovery

The aim of the discovery process was to build a detailed view of the ports and services available from the external IP addresses provided by City of Joondalup. These were firstly scanned using various automated tools. Below is a list of the open ports and services found to be operating on the given targets. Ports are TCP unless otherwise stated:

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 6 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Table 1 – Service Discovery

IP	Ports	Services	Application
103.233.148.130	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	18264	HTTP	Check Point Certificate Services
203.161.120.100	25	SMTP	IronPort
203.161.120.103 api.joondalup.wa.gov.au employment.joondalup.wa.gov.au	80	HTTP	Microsoft HTTPAPI
	443	HTTPS	Microsoft HTTPAPI
203.161.120.104 gis.joondalup.wa.gov.au lodge.joondalup.wa.gov.au www.joondalup.wa.gov.au	80	HTTP	Microsoft HTTPAPI
	443	HTTPS	Microsoft HTTPAPI
203.161.120.105 maps.joondalup.wa.gov.au forms.joondalup.wa.gov.au enews.joondalup.wa.gov.au fileshare.joondalup.wa.gov.au events.joondalup.wa.gov.au jobs.joondalup.wa.gov.au	80	HTTP	Microsoft IIS
	443	HTTPS	Microsoft IIS
	8000	HTTP	Icecast streaming media server
203.161.120.109	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	500(udp)	IKE	
	18264	HTTP	Check Point Certificate Services
203.161.120.113	4786	SMART-INSTALL	Cisco Smart Install
203.161.120.114	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	18264	HTTP	Check Point Certificate Services

IP	Ports	Services	Application
203.161.120.115	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	500(udp)	IKE	
	18264	HTTP	Check Point Certificate Services
203.161.120.116	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	500(udp)	IKE	
	18264	HTTP	Check Point Certificate Services
203.161.120.118 autodiscover.joondalup.wa.gov.au webmail.joondalup.wa.gov.au	443	HTTPS	Microsoft IIS
203.161.120.65	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	500(udp)	IKE	
	18264	HTTP	Check Point Certificate Services
203.161.120.69 docs.joondalup.wa.gov.au	443	HTTPS	Acronis Access
	444	HTTPS	Acronis Access
	3000	HTTPS	Acronis Access
	5787	HTTP	CherryPy
203.161.120.71 m.joondalup.wa.gov.au	80	HTTP	Microsoft IIS
	443	HTTPS	Microsoft IIS
203.161.120.72	25	SMTP	Iron Port
203.161.120.75 view.joondalup.wa.gov.au	80	HTTP	VMware Horizon
	443	HTTPS	VMware Horizon
	4172	PCoIP	
203.161.120.81	22	SSH	Cisco SSH
	443	HTTPS	
	4786	SMART-INSTALL	Cisco Smart Install

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 8 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

IP	Ports	Services	Application
203.161.120.82	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	500(udp)	IKE	
	18264	HTTP	Check Point Certificate Services
203.161.120.97	80	HTTP	Check Point VPN
	264	FW1-TOPOLOGY	Check Point FireWall-1 Topology
	443	HTTPS	Check Point VPN
	18264	HTTP	Check Point Certificate Services
203.161.120.98			
mx2.joondalup.wa.gov.au	25	SMTP	IronPort
mailgwyin1.joondalup.wa.gov.au			

Open sources of intelligence relating to known third-party password breaches such as; Adobe, LinkedIn and Myspace, were investigated for occurrences of the "@joondalup.wa.gov.au" domain name. From this process, 33 accounts were returned with known or reversible passwords.

PDF and Microsoft office documents associated with City of Joondalup were collected using Google and Bing. Analysis of the metadata contained within these documents produced several potential usernames: From the above findings, it was concluded that potential username schemes was most likely <First Name><Last Initial>.

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 9 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

2.4. Attack

The remainder of this section has been split based on the specific application and hosts being targeted.

webmail.joondalup.wa.gov.au

From reviewing version numbers in the OWA page, the version of Microsoft Exchange was identified as Exchange 2013 Cumulative Update 7. This version was released in late 2014 and several vulnerabilities have been identified in Exchange since this time. However, exploitation details which would allow remote access, have not been made publicly available and are not wide spread. This prevented the assessor from progressing further in this instance.

A common vulnerability within OWA was leveraged by the assessor, to determine the internal IP address associated with the host. This process was considered successful, with an IP of 172.20.30.101 returned. Whilst this would be considered helpful to an attacker in certain circumstances, it did not lead to further access or exploitation in this instance.

After this, a known vulnerability within OWA was leveraged to confirm whether an account existed within the related domain (identified to be COJ). Potential account names were identified by using LinkedIn to obtain a current list of employee names and applying the company naming scheme identified in the discovery phase. From this process 61 potential user accounts were identified. Using these names as well as common service account names, a password spray attack was initiated where very common passwords were attempted against each potential account at the rate of 1 attempt per hour. As most domains are configured to lockout users after 5 incorrect guesses and will automatically unlock accounts after 30 minutes, reducing login attempts to 1 guess per hour will typically avoid lockouts. Initial password guessing attempts were successful with two users identified to be using a weak password. Once access to their accounts were verified, their email address books were downloaded and the list of all email addresses were converted to the user naming scheme identified for COJ. From this process 499 accounts were verified for the COJ domain. Further password spraying revealed an additional 4 accounts with very weak passwords.

Table 2 – City of Joondalup Confirmed Credentials

COJ\RyanB	COJ\ChristopherM	COJ\AshlieG
COJ\FrancescaL	COJ\GraceD	COJ\LewisG

Given the potential high risk related to this finding, its presence was communicated to the technical contact, Greg Burgess upon confirmation.

It was indicated that the COJ domain has a lockout policy, after three (3) incorrect password attempts the account was locked out and required an administrator to unlock it. Greg informed ES2 that several accounts had been locked out. Because of this, further password spray attempts were suspended to prevent additional lockouts. It should be noted that users could legitimately mistype their password three (3) times and that this policy may cause users to avoid using complex passwords. The Australian Cyber Security Centre (ACSC) advises that lockout policies can allow five (5) incorrect attempts and for the lockout counter to be reset after as little as 15 minutes and still be effective¹.

¹ https://acsc.gov.au/publications/protect/Hardening_Win10.pdf

Check Point VPN

Once domain account credentials had been obtained, services were reviewed to identify where it may be possible to login to the network. A Check Point VPN interface was identified on several of the hosts within scope of the assessment. Login attempts revealed that the credentials gathered earlier in the assessment would allow a successful connection to the VPN. However, applications had not been configured to work with the gateway and methods to progress further into the network using this connection were not identified within the assessment timeframe.

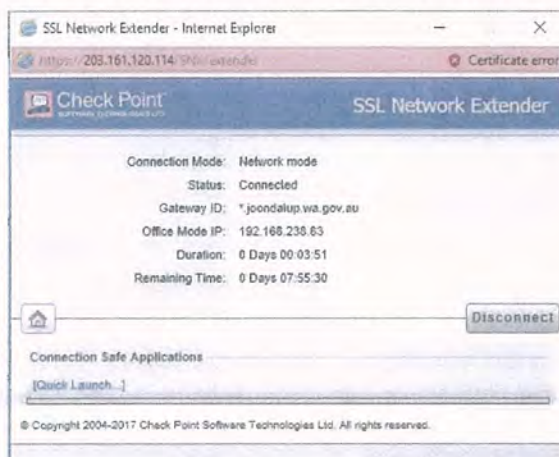


Figure 3 - Check Point Connection

In addition to the Check Point VPN, a VMware Horizons VPN was also identified. However, none of the credentials gathered were permitted to use it. This indicates that only select users are granted remote access, a wise security choice for COJ.

Cisco Smart Install

From external scans the Cisco Smart Install service was identified on two hosts; 203.161.120.81 and 203.161.120.113. Cisco Smart Install allows device configuration to be exported to a remote TFTP server without authentication. As TFTP does not use any form of encryption exploiting this vulnerability would have resulted in the configuration details, including usernames and passwords, being sent over the internet in plaintext. Due to the potential risk that these credentials could be intercepted on exploitation, actual exploitation of the vulnerability was not performed and instead the vulnerability details were communicated to the technical contact, Greg Burgess upon confirmation of the vulnerability.

events.joondalup.wa.gov.au

A WordPress installation was identified at events.joondalup.wa.gov.au. A series of scans were run to identify the WordPress install. From this process the version of WordPress was identified as 4.9.6. It should be noted that there is a known vulnerability for this version of WordPress, which can allow deletion of any file within the WordPress install. However, at the time of writing this report exploitation details are not widely spread or publicly known. Several of the installed WordPress plugins were also identified to be significantly outdated with one WP Maintenance Mode containing multiple vulnerabilities. None of these vulnerabilities were exploited within the time frame of the engagement.

After the patch levels had been assessed a known vulnerability within WordPress was used to enumerate users, leading to "mikethespike", "webuser", "lynleys" and "margaretb" being identified as valid usernames. A public breach database was then searched for past password for each of the

Commercial in Confidence

users. From this process it was identified that “lynleys” was using the same password as in a previous breach.

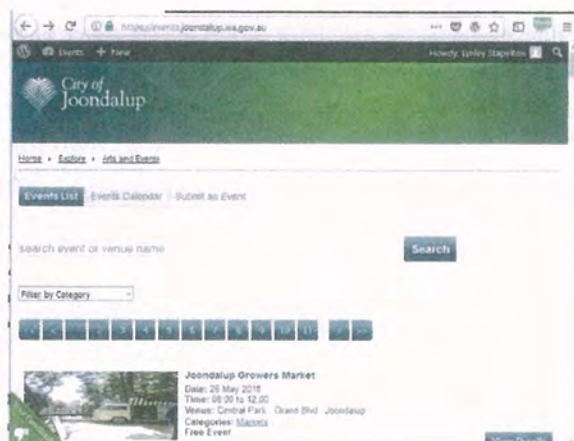


Figure 4 - WordPress Session

After authentication with the identified credentials, it was noted that IIS was filtering several of the URLs typically used to administer WordPress, preventing direct access to the WordPress administration console. While a path to remote code execution was not identified in this instance, it should be noted that URL filters usually do not filter all endpoints and with more time an attacker may be able to use this access to perform malicious actions.

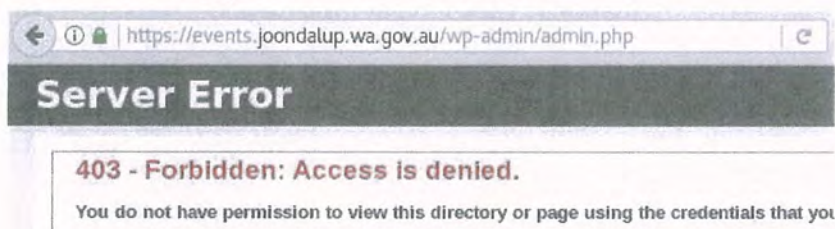


Figure 5 - WordPress Admin Console Filtering

www.joondalup.wa.gov.au and m.joondalup.wa.gov.au

From reviewing the site located at www.joondalup.wa.gov.au it was noted that the site was running Sitefinity 3.7.2136. This version of Sitefinity is significantly outdated and there is a known exploit relating to an insecure image upload². However, to exploit this vulnerability a valid login was required which was not obtained during the engagement time frame.

Flash Cross Domain

From reviewing fileshare.joondalup.wa.gov.au, it was noted that a Cross Domain Flash policy which would allow any flash object from any domain was present. This configuration could be abused by an attacker if they could convince a user to load a link with a malicious flash object, however as user interaction was required this vulnerability was not exploited during the engagement.

² <https://www.exploit-db.com/exploits/15563/>

3. Results and Findings

Overall, 5 high-risk vulnerabilities, were discovered within the external infrastructure, the bulk of these vulnerabilities were related to the use of outdated applications and components, weak passwords and overly permissive policies. An attacker may be able to leverage these issues to compromise either user accounts (through password discovery or exploitation of overly permissive policies) or systems directly (through exploitation of older operation components).

All vulnerabilities have been given a priority categorisation indicator, which is used to represent the potential impact on the business, as well as the time frame recommended for remediation. Category indicators used within this document are as follows:

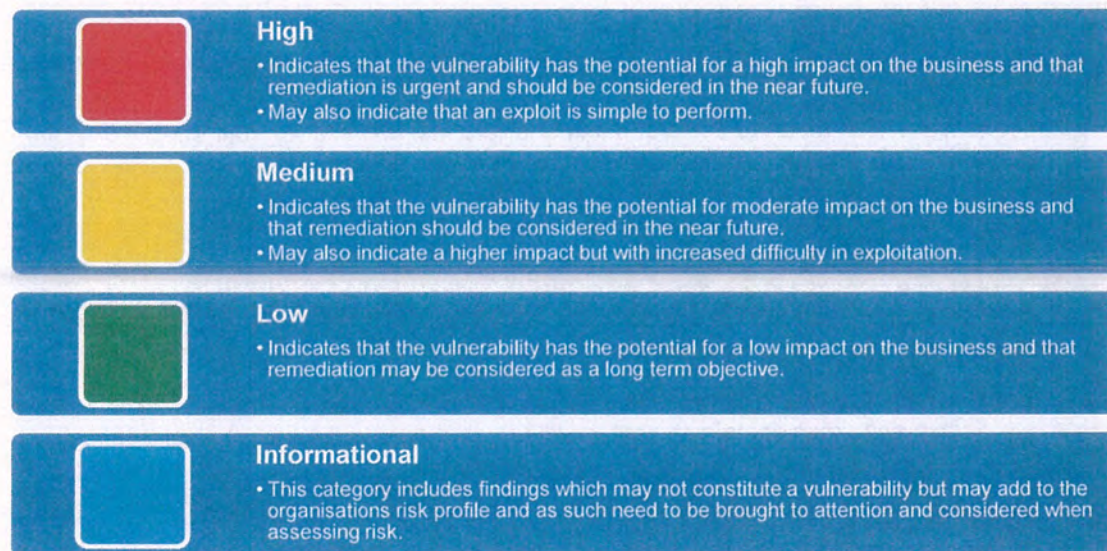


Figure 6 - Severity Scale

3.1. Results Overview

Finding and Suggested Remediation	
H01	Application with Missing Patches Where possible, apply the missing patches to the impacted applications. A focus should be placed on those applications that are considered business critical, and those applications that often interact with untrusted data streams (such as internet facing applications).
	Weak Password Identified Adjust the weak password on impacted accounts. This should prioritise privileged accounts (such as Administrators) and those with certain access rights (such as Remote Desktop). The domain should have its password policy altered to enforce longer passwords, with a minimum length of 10 characters being recommended. A recommendation is also made to conduct security awareness training for staff surrounding the selection of strong passwords. This should include references to the risks of password reuse across different services, avoidance of dictionary words and avoidance of repetition.
H03	(Resolved) Cisco Smart Install Service The solution to the Cisco Smart Install feature is to disable it all together by configuring the service to "no vstack".
H04	Flash Cross Domain allows any Domain Remove the crossdomain.xml file from the affected server if flash or cross domain sharing is no longer required. Alternatively, if flash and cross domain sharing is still required ensure the crossdomain.xml policy document is updated to the domains with which resources need to be shared.
H05	SSH Version 1 Support Disable the SSHv1 service and provide an SSHv2 alternative.
M01	Host accepts SSLv3 Disable support for SSLv3 in favour of at least TLS v1.1. Note that TLS 1.0 should not be considered a secure alternative and should itself be disabled.
M02	Account Lockout Denial of Service Consider increasing the number of incorrect attempts which are permitted to avoid legitimate users locking themselves out. In this specific instance, it is not recommended to apply this finding unless the password complexity is updated (see finding H02). This is due to the fact that the current configuration contains strong defences against password guessing attacks, which is highly recommended given the weak password policy.
M03	Tomcat Management Interface Disable access to the Tomcat management interface for any users or IP addresses that cannot be trusted. It is recommended to only allow access to this interface to internal and trusted clients.
L01	Clickjacking To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY preventing framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 14 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Finding and Suggested Remediation

L02	OWA Internal IP Disclosure Manually set the Realm for any folders configured to support Basic Authentication. Further information can be found at the following resource: http://blog.kurtiskent.com/2014/09/workaround-for-iis-multiple-internal-ip.html
L03	OWA Username Enumeration In this specific instance, no direct solution (such as patching) is available, with the vulnerability itself an accepted risk by the respective developers. Given this, a recommendation is made to ensure strong password selection is undertaken by users, and consideration to the implementation of a second factor of authentication. Alternatively, or additionally, security controls can be placed around the impacted asset, such as a Web Application Firewall or Intrusion Prevention System.
L04	Open Directory Browsing Configured Disable directory browsing for the impacted directories.
L05	Outdated JavaScript Library Update the jQuery library to the latest available version.
L06	PHP Information Disclosure Remove the impacted assets/files.
L07	Strict Transport Security Not Enforced (HSTS) Adjust the application to return the HSTS header, forcing a user's browser to only allow communication via HTTPS. Implementation of this solution can disrupt certain applications, in particular those with mixed-content (i.e. applications that request resources over both HTTP and HTTPS). Given this, a related recommendation is to test this solution prior to implementation into a production environment.

3.2. Detailed Technical Results

H01	Application with Missing Patches	Prioritisation:	HIGH
Description			
Several applications were found to be missing security-related patches, with at least one of these being considered critical for each application.			
Risk			
Depending on the missing patch and related vulnerability, an attacker may be able to achieve information disclosure, account compromise, remote code execution or complete device compromise.			
These findings are based primarily on the self-reported versions of software from the impacted hosts. Occasionally, developers will back port patches to security issues without updating these version numbers. Where and if this has occurred, the current finding may be considered a false positive for that application/component.			
Recommendation			
Where possible, apply the missing patches to the impacted applications. A focus should be placed on those applications that are considered business critical, and those applications that often interact with untrusted data streams such as internet facing applications.			
Impacted Assets			
This finding applies to all applications. However, the following were specifically identified.			
■ www.joondalup.wa.gov.au, m.joondalup.wa.gov.au - Sitefinity ■ 203.161.120.100, 203.161.120.72 - Iron Port ■ events.joondalup.wa.gov.au - WordPress			

H02	Weak Password Identified	Prioritisation:	HIGH
Description			
Password was identified that would be considered weak to certain attacks.			
Risk			
Given the use of password to authenticate users, weak passwords can increase the likelihood of successful attacks against user accounts. This can lead to deeper network access by an attacker, including access to potentially sensitive resources.			
Recommendation			
Adjust the weak password on impacted accounts. This should prioritise privileged accounts (such as Administrators) and those with certain access rights (such as Remote Desktop).			
The domain should have its password policy altered to enforce longer passwords, with a minimum length of 10 characters being recommended.			

A recommendation is also made to conduct security awareness training for staff surrounding the selection of strong passwords. This should include references to the risks of password reuse across different services, avoidance of dictionary words and avoidance of repetition.

Impacted Assets

Remediation for this finding should be applied across organization, however the following accounts were specifically identified during the engagement

- COJ\RyanB
- COJ\ChristopherM
- COJ\AshlieG
- COJ\FrancescaL
- COJ\GraceD,
- COJ\LewisG

H03	(Resolved) Cisco Smart Install Service	Prioritisation:	HIGH
Description			
The Cisco smart install service was detected.			
Risk			
Cisco provides plug and play functionality which allows unauthenticated access. This opens the service to abuse which includes changing configuration files thus causing a major disruption.			
Recommendation			
The solution to the Cisco Smart Install feature is to disable it all together by configuring the service to "no vstack".			
Impacted Assets			
Resolved: 203.161.120.113, 203.161.120.81			

H04	Flash Cross Domain allows any Domain	Prioritisation:	HIGH
Description			
The application publishes a Flash cross-domain policy which allows access from any domain.			
Risk			
Allowing access from all domains means that any domain can perform two-way interaction with this application. Unless the application consists entirely of unprotected public content, this policy is likely to present a significant security risk.			

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 17 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Recommendation
Remove the crossdomain.xml file from the affected server if flash or cross domain sharing is no longer required. Alternatively, if flash and cross domain sharing is still required, ensure the crossdomain.xml policy document is updated to the domains with which resources need to be shared.
Impacted Assets
fileshare.joondalup.wa.gov.au

H05	SSH Version 1 Support	Prioritisation:	HIGH
Description	The server is running an obsolete version of the secure shell service (SSH – Cisco 1.25).		
Risk	SSH version 1 is fundamentally weak and can be successfully attacked with a Man in the Middle approach. This enables a malicious party to compromise the confidentiality of any data that has been encrypted using the SSH version 1 service.		
Recommendation	Disable the SSHv1 service and provide an SSHv2 alternative.		
Impacted Assets	203.161.120.113		

M01	Host accepts SSLv3	Prioritisation:	MEDIUM
Description	A system was found to support version 3 of the SSL protocol, which contains known vulnerabilities relating to encryption and padding.		
Risk	If an attacker is able to position themselves correctly on a network, it may be possible to decrypt portions of the connection, typically leading to account compromise and information disclosure.		
Recommendation	Disable support for SSLv3 in favour of at least TLS v1.1. Note that TLS 1.0 should not be considered a secure alternative, and should itself be disabled.		
Impacted Assets	203.161.120.69 203.161.120.118		

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 18 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

M02	Overly Restrictive Lockout Policy	Prioritisation:	MEDIUM
Description			
A hard lockout mechanism was detected that could allow a legitimate user to lock themselves out even if they knew their password.			
Risk			
Whilst this behaviour is a very strong and effective response to certain attacks, it does itself introduce some vulnerabilities. Where users become averse to setting complex passwords for fear of locking themselves out of their account. In addition, a hard lockout requires avenues to unlock accounts (such as communication with an application administrator). These channels create expectations, in turn increasing the effectiveness and ease of social engineering attacks through this mechanism.			
Recommendation			
Consider increasing the number of incorrect attempts which are permitted to avoid legitimate users locking themselves out. In this specific instance, it is not recommended to apply this finding unless the password complexity is updated (see finding H02). This is due to the fact that the current configuration contains strong defences against password guessing attacks, which is highly recommended given the weak password policy.			
Impacted Assets			
This finding applies across the domain.			

M03	Tomcat Management Interface	Prioritisation:	MEDIUM
Description			
It was possible to attempt access to the management interface of a Tomcat application/server.			
Risk			
If the username and password combination is discovered by an attacker or the authentication process somehow bypassed, it may be possible for an attacker to initiate management-level actions. This can include the uploading of malicious files, which in turn can completely compromise the host, generally resulting in network access by an attacker. Note that it could not be confirmed that full access to the management interface could be achieved, given no attempt was made to bypass or attack the authentication process. As such, this finding contains a low possibility of being a false positive finding.			
Recommendation			
Disable access to the Tomcat management interface for any users or IP addresses that cannot be trusted. It is recommended to only allow access to this interface to internal, trusted clients.			

Impacted Assets

203.161.120.69:3000

L01 Clickjacking

Prioritisation:

LOW

Description

If a page fails to set an appropriate X-Frame-Option or Content-Security-Policy HTTP header, it is possible for a page controlled by an attacker to load that page within an iframe. This enables a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker.

By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defences against cross-site request forgery, and may result in unauthorized actions.

Risk

An attacker may craft a malicious website and insert the legitimate COJ web application in an iFrame, fooling an unsuspecting user into thinking that the website is safe to browse.

Recommendation

To effectively prevent framing attacks, the application should return a response header with the name X-Frame-Options and the value DENY preventing framing altogether, or the value SAMEORIGIN to allow framing only by pages on the same origin as the response itself.

Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

Impacted Assets

203.161.120.69

203.161.120.118

L02 OWA Internal IP Disclosure

Prioritisation:

LOW

Description

An HTTP 1.0 GET request without a Host header specified can be used to return the internal IP address of the OWA server.

Risk

This information may be helpful to an attacker, by slightly increasing their knowledge of the internal network and its infrastructure. This data may be combined with other vulnerabilities to perform more substantial attacks against the network.

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 20 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Recommendation

Manually set the Realm for any folders configured to support Basic Authentication. Further information can be found at the following resource:

<http://blog.kurtiskent.com/2014/09/workaround-for-iis-multiple-internal-ip.html>

Impacted Assets

webmail.joondalup.wa.gov.au

L03 OWA Username Enumeration

Prioritisation:

LOW

Description

It was possible to test the validity of usernames via certain requests to an Outlook Web Application (OWA) instance.

Risk

This vulnerability allows an attacker to determine the existence of usernames, increasing the chances of threats related to brute force and dictionary attacks. This in turn increases the likelihood of account compromise, leading to information disclosure and deeper network and/or application penetration by an attacker.

Recommendation

In this specific instance, no direct solution (such as patching) is available, with the vulnerability itself an accepted risk by the respective developers. Given this, a recommendation is made to ensure strong password selection is undertaken by users, and consideration to the implementation of a second factor of authentication.

Alternatively, or additionally, security controls can be placed around the impacted asset, such as a Web Application Firewall or Intrusion Prevention System.

Impacted Assets

webmail.joondalup.wa.gov.au

L04 Open Directory Browsing Configured

Prioritisation:

LOW

Description

A directory was found to be open to browsing.

Risk

Open Directory browsing allows retrieval of all resources within folders, often increasing the knowledge available to an attacker. This increases the likelihood of both vulnerability identification and exploitation.

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 21 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Recommendation
Disable directory browsing for the impacted directories.
Impacted Assets
api.joondalup.wa.gov.au

L05	Outdated JavaScript Library	Prioritisation:	LOW
Description			
Versions for several jQuery-related JavaScript libraries were identified that contain known vulnerabilities, including jQuery-ui-dialog (1.11.1) and jQuery-migrate (1.1.1).			
Risk			
The vulnerability itself increases the likelihood of a successful cross site scripting vulnerability, in certain circumstances. It should be noted that the vulnerability requires very specific circumstances to exploit, and no instance was identified where this vulnerability was exploitable. For the application itself to be considered vulnerable, a specific section of a vulnerable library will need to be referenced and used by the application. Given this, the current finding contains a high likelihood of being a false positive, and as such, has not been included in final vulnerability counts. This should be taken into consideration when determining potentially application of remediation advice.			
Recommendation			
Update the JQuery library to the latest available version.			
Impacted Assets			
203.161.120.105			

L06	PHP Information Disclosure	Prioritisation:	LOW
Description			
A default, informational file relating to PHP was identified on the hosts, containing potentially sensitive information.			
Risk			
The PHP Info file typically contains detailed information relating to the PHP installation, as well as the related host. This information includes internal IP addresses, loaded modules and specific software versions. Access to this information will slightly increase the likelihood of vulnerability discovery and exploitation.			
Recommendation			
Remove the impacted assets/files.			

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 22 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.

Impacted Assets	
enews.joondalup.wa.gov.au	events.joondalup.wa.gov.au

L07	Strict Transport Security Not Enforced (HSTS)	Prioritisation:	LOW
Description			
The application was not found to return a Strict-Transport-Security header during communications.			
Risk			
The Strict-Transport-Security header (HSTS) can help to mitigate several attacks related to downgrade or removal of TLS/SSL based encryption. Failure to implement the header slightly increases the success likelihood of these types of attacks, in turn slightly increasing the likelihood of sensitive information disclosure or account compromise.			
Recommendation			
Adjust the application to return the HSTS header, forcing a user's browser to only allow communication via HTTPS.			
Implementation of this solution can disrupt certain applications, in particular those with mixed-content (i.e. applications that request resources over both HTTP and HTTPS). Given this, a related recommendation is to test this solution prior to implementation into a production environment.			
Impacted Assets			
www.joondalup.wa.gov.au			

IN01	Prioritisation:	INFORMATIONAL
Description		
During testing it was noted that Check Point FireWall-1 Topology reveals hostnames of the relevant devices prior to authentication.		
If this function is not needed by CoJ then ES2 recommends that it is disabled.		

4. Next Steps

Following the results and outcomes of the assessment process, ES2 suggests the following goals for future development of City of Joondalup's externally facing infrastructure:

- Continue with proactive testing and assessment;
- Consider a Password Review for users, as well education on the importance of secure password section; and
- Review and update current patch management policy and implementation.

Definition of Terms and Acronyms

Term/Abbreviation	Meaning
DoS	Denial of Service attack
FTP	File Transfer Protocol
GUI	Graphical User Interface
HSTS	HTTP Strict Transport Security
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IIS	Internet Information Service
OWA	Outlook Web Application/Access
OWASP	Open Web Application Security Project
RDP	Remote Desktop Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
WAF	Web Application Firewall

End

Commercial in Confidence

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ Copyright 2014. All Rights Reserved.
 ES2 - City of Joondalup - External Penetration Test Report ■ Ref: 18-WA-COJ-SE-6

Page 25 of 25

ES2 Pty. Ltd. ■ ABN: 57 163 419 136 ■ www.es2.com.au

This document is the property of ES2 Pty. Ltd. and may not be reproduced or transmitted in whole or in part by any means without written permission.