Building Telco Businesses

CINDY and Network Infrastructure Penetration Test Report

27 November 2017 Version: 1.1

Prepared by: George Stewart

Table of Contents

Executive Summary

Building Telco Businesses (BTB) commissioned Colman Communciations to perform a penetration test against CINDY and network infrastructure. The objective of the penetration test was to assess the effectiveness of BTB's preventative controls against attack by an adversary with credentials to CINDY, but not any other infrastructure.

Testing was conducted between 23 October 2017 and 6 November 2017.

Report findings and vulnerability summary

The key findings of the penetration test were:

1. An unauthenticated remote code execution vulnerability was discovered in the CINDY application.
2. The CINDY application was hosted jointly in a cloud instance and on the internal network. There were no controls enforcing network segregation between the internally hosted instance and the workstations on the internal network.
3. Colman Communciations was able to establish domain dominance once a foothold on the internal network had been established.

Below is an overview of the vulnerabilities identified by Colman Communciations during testing, grouped by priority:

Urgent	High	Medium	Low	Optional
2	4	3	1	3

A total of 22 treatments have been recommended to address them.

Systemic analysis and recommendations

A critical vulnerability was discovered allowing remote unauthenticated code execution. This was caused by the usage of the struts framework version 1, which has an unpatched vulnerability that will never be addressed as the framework has been marked "end of life". In addition to this, a list of other libraries and and their versions indicate that apache-common-collections version 3.1 is in use. This library suffers from a critical de-serialisation flaw that can result in remote code execution. However, checks of the application for evidence of serialised objects passed to the browser did not turn up any results.

> R1. Update application development practices to require the use of up-to-date components.
> R2. Integrate a tool to monitor libraries for vulnerabilities into the build and deploy process, so that vulnerable libraries can not be pushed into production. One such open source tool is OWASP Dependency Check.

Escalation to domain administrator privileges was made possible through the use of missing authentication, default credentials and password reuse. It is likely that had these issues not been discovered, Colman Communciations would not have been able to achieve domain dominance within the test window. It was noted that BTB seems to have a strong password policy, and it is unlikely that any passwords would have been cracked if attempted.

> R3. Ensure that deployment processes require all devices have default credentials changed prior to deployment.
> R4. Encourage the use of password managers to avoid password re-use.
> R5. Reset all credentials identified in this report including credentials for the btb.local domain and KRBTGT account (which must be reset twice in quick succession). The resource https://adsecurity.org/?p=483 provides background into the operation and the resource https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51 contains a script that can assist with the process.

Colman Communciations did not observe an Active Directory design that aligns with best practice. Everyday use accounts of executives had been given domain administrator privileges, and groups to support role based access control were not observed.

R6. Review the Active Directory architecture against Microsoft best-practice.

Introduction

The objective of the penetration test was to assess the effectiveness of BTB's preventative controls against attack by an adversary with credentials to CINDY, but not any other infrastructure.

Timeframe

10 days of testing were allocated for this engagement. The testing was performed between 23 October 2017 and 6 November 2017.

Scope

The test scope was:

- A penetration test of CINDY.
- A penetration test of Internet facing infrastructure.
- A penetration test of the internal networks.

Further information can be found in the test plan btb_2017_test_plan_v1.1.pdf.

Personnel

The following individuals were involved in the testing process:

Name	Role	Phone	Email
George Stewart	Security Tester	0432 918 830	george.stewart@colmancomm.com
Sachin Patel	GM - Product & Technology	0411 655 405	sachin@btbaustralia.com.au
Graham Corrigan	GM - Software and Architecture	0409 368 903	graham@btbaustralia.com.au
Clem Colman	Security Consultant	0417 744 511	clem@colmancomm.com

Setup

Testing of CINDY was performed in a environment dedicated to the penetration test. All other testing was performed in production.

The testing was conducted with limited knowledge of the target. The following was supplied:

- Test accounts for CINDY.
- Libraries in use by CINDY.
- Network diagrams for the organisation.
- An error checking feature that would disable the application for an IP after a certain threshold of errors was hit was disabled.
- Once code execution in CINDY was proven, VPN access to the internal network was provided so that testing could continue without affecting production.

Vulnerabilities

Summary

Description	Rating	Status
Vulnerable libraries in use	Urgent	Partial
Application vulnerable to Cross Site Request Forgery	Urgent	Fixed
Insecure credit card storage and encryption	High	Fixed
Missing/Default passwords	High	Untested
Domain Privileges	High	Untested
Xml Injection	High	Fixed
Poor password security policy	Medium	Fixed
Functions vulnerable to SQL injection	Medium	Fixed
XML External Entity Injection	Medium	Fixed
Missing HTTP headers	Low	Fixed
IP whitelisting not in place as stated	Optional	Untested
Business Logic Error	Optional	Untested
Application infrastructure can be fingerprinted	Optional	Fixed

Ratings

Vulnerabilities are rated on the urgency to fix based off a combination of the ease of exploit, impact if exploited and Colman Communciations's cyber security experience.

- Urgent: The vulnerability is so severe it puts BTB at an immediate unacceptable risk and should be fixed immediately.
- High: The vulnerability will likely put BTB at an unacceptable risk, and should be fixed as quickly as practical.
- Medium: The vulnerability may become a serious threat to BTB, especially if combined with another. It is recommended that the vulnerability be fixed as part of the next release/change window.
- Low: The vulnerability is not likely to become a serious threat to BTB. It is recommended that the vulnerability be fixed as part of a future release as convenient.
- Optional: The vulnerability is unlikely to pose even a low threat to BTB, but has been included for the sake of completeness or because it is part of best practice. BTB can use its discretion when deciding if to remediate.

Vulnerability statuses have been marked based on the results of retesting:

- **Fixed**: fixes for the vulnerability have been tested and confirmed effective.
- **Partial**: a partial or temporary fix has been put in place. A complete fix could not be implemented before completion of the engagement.
- **Untested**: the vulnerability could not be retested before the completion of the engagement.

Document Management

Filename

btb_2017_test_report_v1.1.pdf

Change History

Version	Date	Author	Change Description
0.1	10 November 2017	George Stewart	Draft complete
0.2	12 November 2017	Clem Colman	Internal QA
1.0	13 November 2017	George Stewart	Initial release to client
1.1	27 November 2017	George Stewart	Update with feedback from client and retest results

Referenced Documents

Title	Filename	Version
Network Overview	Network Overview.pdf	17/10/2017
Marketing Material	Origin_Final_v2_email.pdf	2
CINDY and Network Infrastructure Penetration Test Plan	btb_2017_test_plan_v1.1.pdf	1.1

Disclaimer

Colman Communciations notes that penetration tests are limited in a number of aspects:

- They are conducted with limited resources over a limited period of time. An attacker may not face the same constraints.
- They are a point in time assessment. Changes to the security landscape including the discovery of new vulnerabilities, attack techniques, and changes in BTB's environment may lead to new vulnerabilities over time.
- They are performed in a specific environment. There may be differences in configuration between the environment assessed and others.

As a result, Colman Communciations gives no guarantee, warranty, or assurance that the services it has performed and provided pursuant to the assessment will have the effect of:

- Identifying an exhaustive list of all threats and risks to the BTB's systems;
- Documenting all possible controls that might be applied to remediate identified threats and risks; and or
- Being continually accurate and relevant as threats and risks as identified by the Vendor (and any recommended controls) may be time specific.

Threats and risks to assessed systems and controls that have been implemented to remediate such risks and threats should be reviewed regularly to ensure their currency and efficacy.