



...making excellence a habit.™

Dragon Infosec Ltd  
**Temtum iOS Application Security Assessment**

BSI Reference: CSIRUKPRJ-372-RPT-01

Version: 1.0

**1<sup>st</sup> March 2019**

**Testing Team**

Michael Poultsakis (CTL)



## Document Control Information

### 1.1 Document Details

Property	Value
<b>Client</b>	Dragon Infosec Ltd
<b>Title</b>	Dragon Infosec Ltd Temtum iOS Application Security Assessment
<b>Author</b>	Michael Poultzakis
<b>Version</b>	1.0
<b>Date</b>	01/03/2019
<b>Document Reference</b>	CSIRUKPRJ-372-RPT-01
<b>Status</b>	Final

### 1.2 Revision History

Version	Date	Author	Summary of Changes
0.1	01/03/2019	Michael Poultzakis	Initial Draft
0.2	01/03/2019	Brett Thomas	Internal QA
1.0	01/03/2019	Brett Thomas	Definitive Issue

### 1.3 Approvals

Name	Organisation	Role
Peter Viranyi	BSI Cybersecurity and Information Resilience	Head of Security Testing

### 1.4 Distribution

Name	Organisation	Role
Peter Viranyi	BSI Cybersecurity and Information Resilience	Head of Security Testing
Richard Dennis	Dragon Infosec Ltd	Chief Technology Officer

# Table of Contents

- DOCUMENT CONTROL INFORMATION..... 2**
  - 1.1 Document Details .....2
  - 1.2 Revision History .....2
  - 1.3 Approvals.....2
  - 1.4 Distribution .....2
- 2 EXECUTIVE SUMMARY ..... 4**
- 3 INTRODUCTION ..... 5**
  - 3.1 Background.....5
  - 3.2 Approach .....5
  - 3.3 Scope .....5
- 4 TEMTUM MOBILE APPLICATION ASSESSMENT ..... 6**
  - 4.1 No Jailbreak Detection .....6
  - 4.2 Unencrypted Local Cached Data .....7
  - 4.3 Lack of Certificate Pinning .....8
- 5 SERVER BUILD REVIEW ..... 9**
  - 5.1 Missing Ubuntu Patches .....9
  - 5.2 Unix Hardening Improvements .....11
- 6 DATABASE REVIEW ..... 12**
  - 6.1 MongoDB Hardening Improvements.....12
- 7 SUMMARY OF FINDINGS ..... 14**
  - 7.1 Temtum Mobile Application Assessment .....14
  - 7.2 Server Build Review .....15
  - 7.3 Database Review .....16
- APPENDIX A - TESTING TEAM ..... 17**
- APPENDIX B – UNIX HARDENING ..... 18**
- APPENDIX C - FINDINGS DEFINITIONS..... 26**

## 2 Executive Summary

BSI Cybersecurity and Information Resilience were engaged by Dragon Infosec Ltd to perform a penetration test against the iOS version of the Temtum mobile application. Testing was undertaken between the 18<sup>th</sup> and 22<sup>nd</sup> February 2019.

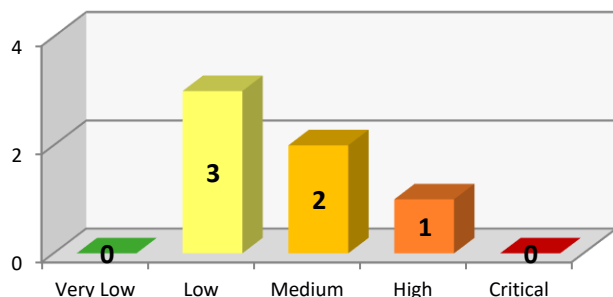
The assessment was performed with the use of a jailbroken device and an intercepting proxy in order to capture, read and modify the traffic. This means that the application did not implement those security controls that otherwise would detect such environments and would prevent the establishment of connections with unauthenticated endpoints (jailbreak detection, certificate pinning).

The review of the application did not reveal the presence of any significant issues that would suggest immediate action. The review of the mechanisms behind user authentication and session management did not indicate any flaws. The application made use of tokens (JWT) instead of session identifiers and ensured that adequate session protection exists in the manner of session expiration, session replay etc.

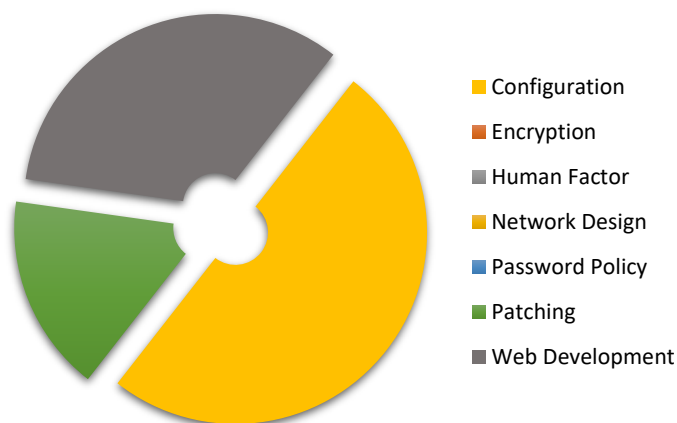
Despite the above, sensitive data was maintained in unencrypted format and could therefore be disclosed to attackers with physical access to the device, or malicious applications, should the application be used on a jailbroken device.

The wallet server (Ubuntu 18.04) was found to be missing a number of important security patches that address vulnerabilities which can lead to a number of attack outcomes, including server compromise. For this reason, it is recommended that the server environment is maintained with all security fixes installed to ensure resilience against known vulnerabilities.

The MongoDB instance was only locally accessible. This was found to be open with no authentication necessary and was immediately fixed immediately after escalation.



This graph illustrates the level of risk that is exposed across the systems tested. It shows the number of vulnerabilities identified during this assessment along with their severity.



This graph shows the distribution of risk within the environment. It is useful to get a sense of the proportion of higher risk issues that need immediate attention.

## **3 Introduction**

### **3.1 Background**

BSI Cybersecurity and Information Resilience were engaged by Dragon Infosec Ltd to perform an assessment against the iOS version of the Temtum wallet application. This followed the assessment that was previously performed against the Android version of the Temtum application. Testing was undertaken between the 18<sup>th</sup> and 22<sup>nd</sup> February 2019.

### **3.2 Approach**

All testing was carried out using BSI Cybersecurity and Information Resilience standard testing methodology. A full copy of this methodology can be provided on request.

### **3.3 Scope**

The scope of the engagement was as follows:

- iOS Mobile Application Assessment - Temtum Application
- Wallet Server Build Review (Ubuntu)
- MongoDB build review

#### **3.3.1 Limitations**

The following limitations were identified:

- BSI does not perform exploitation of vulnerabilities that may impact upon service availability or stability due to the live nature of systems.

## 4 Temtum Mobile Application Assessment

### 4.1 No Jailbreak Detection

Finding No 1.	Systems Affected	Temtum iOS Application		
	Finding	The application was found to run on a Jailbroken iOS device.		
	CVE Number	N/A		
	Root Cause	<b>Web Development</b>		
	Impact	<b>3</b>		
	Likelihood	<b>3</b>		
	Overall Risk Rating	<b>9 (Medium Risk)</b>		
	Status	<b>ONGOING</b>		

#### 4.1.1 Summary

The process of jailbreaking of an iOS device results in an increased level of access to the underlying operating system for the user, thus, putting the components of the application at increased risk of compromise. Additionally, jailbreaking or rooting often decreases the security posture of a device, meaning that the application and its data could be compromised by other malicious application or malicious users.

#### 4.1.2 Technical Details

It was identified that the mobile application did not employ robust controls to prevent it from being successfully run on jailbroken devices.

Despite the above, the application was found to employ mechanisms to identify a jailbroken environment, as indicated by the contents of the below file:

`\Library\Caches\com.crashlytics.data\com.effective-soft.Temtum\analytics\v2\crash_metadata`

```
{
  "platform_code": 1,
  "generator": "Answers",
  "bundle_version": "1",
  "machine": "iPhone8,4",
  "api_key": "cf7182c247252ac7bf7691393934f6433c3a894e",
  "jailbroken": true,
  "cores": 2,
  "bundle_id": "com.effective-soft.Temtum",
  "instance_id": "f6c64533cba795dfea91cd6f17ead7f4214d3279",
  "locale": "en_IE",
  "bundle_short_version": "1.0",
  "platform": "iOS",
  "os_build": "14B100",
  "started_at": 1550764140,
  "install_id": "59A49AFB-02B3-4CC8-A11A-CE1BA79B78E7",
  "session_id": "c9100fdab5a6486b9bf745b7730e3eaa",
  "model": "iPhone8,4",
  "os_version": "10.1.1"
}
```

#### 4.1.3 Recommendation

BSI recommends that the application performs root checking at run time.

## 4.2 Unencrypted Local Cached Data

Finding No 2.	Systems Affected	Temtum iOS Application		
	Finding	The local SQLite database that maintained data locally was not encrypted.		
	CVE Number	N/A		
	Root Cause	<b>Configuration</b>		
	Impact	<b>4</b>		
	Likelihood	<b>2</b>		
	Overall Risk Rating	<b>8 (Medium Risk)</b>		
	Status	<b>ONGOING</b>		

### 4.2.1 Summary

The application made use of a local SQLite database to persistently maintain application data such as transaction and user information between different application runs.

### 4.2.2 Technical Details

SQLite is an open-source embedded database engine that stores data within a flat file. It is possible to access the database contents by pulling the file out of the device and then read its contents.

Due to the ease of access, it is recommended that sensitive information is adequately protected from access with the use of encryption.

The below screenshot, illustrates how data is stored in unencrypted format, allowing an attacker or malicious application to access it.

```

root@kali:~/projects/tem# sqlite3 DataStorage.sqlite
SQLite version 3.26.0 2018-12-12 11:57:35
Enter ".help" for usage hints.
sqlite> show tables
...>
Error: near "show": syntax error
sqlite> .tables
ZFAQ          ZTRANSACTION  ZUSERDEVICE   Z_PRIMARYKEY
ZGOOGLEAUTH  ZTRANSACTIONUSER Z_METADATA
ZLOGINHISTORY ZUSER         Z_MODELCACHE
sqlite> select * from ZTRANSACTION
...>
12|4|1|3|2|2|1|d49c92b770dd9dde9dc19e320e5196a1045071eb37942a6b83b004b258d3860b|2019-02-21T14:16:20.020Z|5c6eb2b4c823ba602fba374c|XXXX">|
13|4|1|100|2|1|2|d5cbd0d6f0930a2a6cd4bfff6562c8c19986ed79cd3a7ae0b350f6b60b08aff26|2019-02-18T17:06:32.177Z|5c6ae61861f55d4a870514ec|for Michael|
14|4|1|1000|2|3|2|1a97e237f0d82ca001f25ee96da723d2fbfa3afeab3683ab24746c1b87e97990|2019-02-20T17:31:26.954Z|5c6d8eeec823ba602fba3745||
15|4|1|4|2|2|2|e4b90cb398020db3765a6f736750edcc2794ad3f16271215e0df7c6db61c514d|2019-02-21T14:46:16.959Z|5c6eb9b8c823ba602fba3751|Xxx|
16|4|1|1|2|2|1|caa4de3b2782c200fc5e3983d6149752edad1b39185fec649cf7dba8f1884589|2019-02-21T14:54:19.230Z|5c6ebb9bc823ba602fba3752|XXX111|
    
```

Figure 1 - unencrypted local database

### 4.2.3 Recommendation

BSI recommends that data encryption is used to protect the data stored or sensitive session data is not stored within the database.

### 4.3 Lack of Certificate Pinning

Finding No 3.	Systems Affected	Temtum iOS Application		
	Finding	The application did not employ any server authenticity checks and it was therefore possible to intercept its traffic through the use of an intercepting proxy.		
	CVE Number	N/A		
	Root Cause	<b>Web Development</b>		
	Impact	2		
	Likelihood	2		
	Overall Risk Rating	<b>4 (Low Risk)</b>		
	Status	<b>ONGOING</b>		

#### 4.3.1 Summary

It was possible to intercept all HTTPS traffic by configuring the device to use an attacker-controlled proxy server.

#### 4.3.2 Technical Details

The application accepted to connect and communicate with any untrusted server. As a result, it was possible to configure the device to use an intermediate proxy which acted as an SSL termination point as well as a new SSL client for the rest of the connection, effectively allowing the attacker to intercept, replay and tamper all application traffic.

It is however, common practice for mobile applications to refuse to connect if the server certificate does not match an existing set of pre-configured signatures, effectively preventing the send traffic in the presence of a possible intercepting proxy.

#### 4.3.3 Recommendation

It is recommended that certificate pinning is enforced. This is achieved by providing the application with a list of whitelisted server public keys. The application should refuse to communicate if an unknown public key is returned by the remote server.



Certificate pinning prevents attacker from decrypting SSL/TLS traffic.

[https://www.owasp.org/index.php/Certificate\\_and\\_Public\\_Key\\_Pinning](https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning)



## 5 Server Build Review

### 5.1 Missing Ubuntu Patches

Finding No 4.	Systems Affected	wallet.temtum.com (54.38.214.253)
	Finding	The Ubuntu operating system was found to be missing multiple security updates.
	CVE Number	N/A
	Root Cause	<b>Patching</b>
	Impact	<b>4</b> 
	Likelihood	<b>3</b> 
	Overall Risk Rating	<b>12 (High Risk)</b>
	Status	<b>ONGOING</b>

#### 5.1.1 Summary

Multiple security patches were identified as missing from the wallet.temtum.com Ubuntu server. An attacker with the appropriate network access could exploit an existing vulnerability to perform a series of attacks, including denial of service, privilege escalation or even remotely compromise the system by exploiting a remote execution vulnerability.

#### 5.1.2 Technical Details

The following Ubuntu security patches were identified as missing:

Patch ID	Risk	Date	Description
USN-3887-1	High	12/02/2019 <small>(17 days old)</small>	Installed package: snapd_2.32.8+18.04 Fixed package: snapd_2.34.2+18.04.1
USN-3882-1	High	06/02/2019 <small>(23 days old)</small>	Installed package: curl_7.58.0-2ubuntu3.5 Fixed package: curl_7.58.0-2ubuntu3.6  Installed package: libcurl3-gnutls_7.58.0-2ubuntu3.5 Fixed package: libcurl3-gnutls_7.58.0-2ubuntu3.6  Installed package: libcurl4_7.58.0-2ubuntu3.5 Fixed package: libcurl4_7.58.0-2ubuntu3.6
USN-3871-2	High	31/01/2019 <small>(29 days old)</small>	Installed package: linux-image-4.15.0-43-generic_4.15.0-43.46 Fixed package: linux-image-4.15.0-45-generic_4.15.0-45.48
USN-3871-1	High	29/01/2019 <small>(31 days old)</small>	Installed package: linux-image-4.15.0-43-generic_4.15.0-43.46 Fixed package: linux-image-4.15.0-44-generic_4.15.0-44.47
USN-3863-1	High	22/01/2019 <small>(38 days old)</small>	Installed package: apt_1.6.3ubuntu0.1 Fixed package: apt_1.6.6ubuntu0.1

USN-3861-1	High	16/01/2019 <small>(44 days old)</small>	Installed package: libpolkit-backend-1-0_0.105-20ubuntu0.18.04.1 Fixed package: libpolkit-backend-1-0_0.105-20ubuntu0.18.04.4  Installed package: policykit-1_0.105-20ubuntu0.18.04.1 Fixed package: policykit-1_0.105-20ubuntu0.18.04.4
USN-3885-1	Medium	07/02/2019 <small>(22 days old)</small>	Installed package: openssh-client_1: 7.6p1-4ubuntu0.1 Fixed package: openssh-client_1: 7.6p1-4ubuntu0.2
USN-3855-1	Medium	11/01/2019 <small>(49 days old)</small>	Installed package: systemd_237-3ubuntu10.9 Fixed package: systemd_237-3ubuntu10.11
USN-3853-1	Medium	10/01/2019 <small>(50 days old)</small>	Installed package: gnupg_2.2.4-1ubuntu1.1 Fixed package: gnupg_2.2.4-1ubuntu1.2  Installed package: gpg-wks-client_2.2.4-1ubuntu1.1 Fixed package: gpg-wks-client_2.2.4-1ubuntu1.2

**Table 1 - Missing Ubuntu patches on vps544591 (54.38.214.253)**

### 5.1.3 Recommendation

BSI recommends that the system be updated to ensure that all security related package updates issued by the vendor are installed.


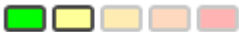
This can be accomplished by executing the following commands:

```
sudo apt-get update
sudo apt-get upgrade
```

The following command can be used to determine what actions the package manager will perform before actually updating the system:

```
sudo apt-get upgrade -s
```

## 5.2 Unix Hardening Improvements

Finding No 5.	Systems Affected	wallet.temtum.com (54.38.214.253)
	Finding	The hardening level of the server under review was found to be in need of further improvements.
	CVE Number	N/A
	Root Cause	<b>Configuration</b>
	Impact	2 
	Likelihood	2 
	Overall Risk Rating	<b>4 (Low Risk)</b>
	Status	<b>ONGOING</b>

### 5.2.1 Summary

The server under review was in need of a number of configuration improvements to reach a satisfactory level of reduced attack surface and hardening.

### 5.2.2 Technical Details

The table in Appendix B lists the settings that could benefit from further hardening.

### 5.2.3 Recommendation

Consider implementing the above listed changes to reduce system exposure.

## 6 Database Review

### 6.1 MongoDB Hardening Improvements

Finding No 6.	Systems Affected	wallet.temtum.com (54.38.214.253)
	Finding	A number of configuration changes were found to be required in order to reach a satisfactory level of MongoDB hardening.
	CVE Number	N/A
	Root Cause	<b>Configuration</b>
	Impact	2
	Likelihood	2
	Overall Risk Rating	<b>4 (Low Risk)</b>
	Status	<b>ONGOING</b>

#### 6.1.1 Summary

The MongoDB installation was found to require further configuration changes in order to achieve a reduced attack surface.

#### 6.1.2 Technical Details

The following table lists the hardening steps that are required to further enhance the security posture of the MongoDB installation.

Policy	Current Setting
Ensure that database file permissions are set correctly	The file /var/lib/mongodb with fmode owner: mongodb group: mongodb mode: 0755 attr: -----e--- uid: 111 gid: 115 uneven permissions : FALSE does not match the policy value owner: mongodb group: mongodb mask: 0117 uneven permissions : TRUE  /var/lib/mongodb
Ensure that key file permissions are set correctly	No keyfile present
Ensure that audit filters are configured properly	The command 'cat /etc/mongod.conf  grep -A4 'auditLog'   grep 'filter' did not return any result
Ensure that system activity is audited	The command 'cat /etc/mongod.conf grep -A4 'auditLog'   grep 'destination' did not return any result
Ensure Federal Information Processing Standard (FIPS) is enabled	The command 'cat /etc/mongod.conf   grep -A20 'net'   grep -A10 'ssl'   grep 'FIPMode' did not return any result
Ensure TLS or SSL protects all network communications	The command 'cat /etc/mongod.conf   grep -A20 'net'   grep -A10 'ssl'   grep 'mode' did not return any result
Ensure that MongoDB is run using a non-privileged, dedicated service account	The command 'ps -ef   grep -E mongos mongod' returned :  mongodb 779 1 0 2018 ? 08:17:26 /usr/bin/mongod --config /etc/mongod.conf bsi 17040 16935 0 15:25 ? 00:00:00 bash -c LANG=C; ps -ef   grep -E mongos mongod cat

	bsi 17042 17040 0 15:25 ? 00:00:00 grep -E mongos mongod
Ensure authentication is enabled in the sharded cluster	No keyFile set. The file /etc/mongod.conf does not contain ^[\s]*keyFile[\s]*=

**Table 2 - UNIX failed compliance onvps544591 (54.38.214.253)**

### **6.1.3 Recommendation**

BSI recommends that the listed configuration changes are implemented.

## 7 Summary of Findings

### 7.1 Temtum Mobile Application Assessment

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
1	3	3	Medium	<b>No Jailbreak Detection</b> The application was found to run on a Jailbroken iOS device.	BSI recommends that the application performs root checking at run time.	<b>ONGOING</b>
2	4	2	Medium	<b>Unencrypted Local Cached Data</b> The local SQLite database that maintained data locally was not encrypted.	BSI recommends that data encryption is used to protect the data stored or sensitive session data is not stored within the database.	<b>ONGOING</b>
3	2	2	Low	<b>Lack of Certificate Pinning</b> The application did not employ any server authenticity checks and it was therefore possible to intercept its traffic through the use of an intercepting proxy.	It is recommended that certificate pinning is enforced. This is achieved by providing the application with a list of whitelisted server public keys. The application should refuse to communicate if an unknown public key is returned by the remote server.	<b>ONGOING</b>

## 7.2 Server Build Review

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
4	4	3	High	<b>Missing Ubuntu Patches</b> The Ubuntu operating system was found to be missing multiple security updates.	BSI recommends that the system be updated to ensure that all security related package updates issued by the vendor are installed.	<b>ONGOING</b>
5	2	2	Low	<b>Unix Hardening Improvements</b> The hardening level of the server under review was found to be in need of further improvements.	Consider implementing the above listed changes to reduce system exposure.	<b>ONGOING</b>

### 7.3 Database Review

Finding No.	Impact	Likelihood	Overall Risk	Finding	Recommendation	Status
6	2	2	Low	<p><b>MongoDB Hardening Improvements</b></p> <p>A number of configuration changes were found to be required in order to reach a satisfactory level of MongoDB hardening.</p>	BSI recommends that the listed configuration changes are implemented.	<b>ONGOING</b>



## **Appendix A - Testing Team**

This project was undertaken using the following consultants:

- Michael Poultsakis (CTL)

Any queries regarding this testing and report should be directed to:

BSI Cybersecurity and Information Resilience Operations Team

Tel: +44 (0) 345 222 1711

Email: [Operations.Cyber.UK@bsigroup.com](mailto:Operations.Cyber.UK@bsigroup.com)

The primary point of contact at Dragon Infosec Ltd was Richard Dennis ([Richard@dragoninfosec.com](mailto:Richard@dragoninfosec.com)).

**Appendix B – UNIX Hardening**

The below table lists the items that were found to require additional hardening.

Policy and Recommendation	Current Setting
Ensure remote rsyslog messages are only accepted on designated log hosts - '\$InputTCPServerRun 514' - rsyslog.conf/rsyslog.d	The command '/bin/grep '^s*\\$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
Ensure remote rsyslog messages are only accepted on designated log hosts - '\$ModLoad imtcp.so' - rsyslog.conf/rsyslog.d	The command '/bin/grep '^s*\\$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
Ensure rsyslog is configured to send logs to a remote log host - rsyslog.conf/rsyslog.d.	The command 'grep '^*.[^I][^I]*@' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'local6,local7.* -/var/log/localmessages'	The command '/bin/grep '^s*local6,local7' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'local4,local5.* -/var/log/localmessages'	The command '/bin/grep '^s*local4,local5' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'local2,local3.* -/var/log/localmessages'	The command '/bin/grep '^s*local2,local3' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'local0,local1.* -/var/log/localmessages'	The command '/bin/grep '^s*local0,local1' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - '*.*;mail.none;news.none - /var/log/messages'	The command '/bin/grep '^s*\\.*;mail.none;news\\.none' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - '*.*crit /var/log/warn'	The command '/bin/grep '^s*\\.*.crit' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - '*.*=warning;*.err -/var/log/warn'	The command '/bin/grep '^s*\\.*.=warning;\\.*.err' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
logging is configured - 'news.notice - /var/log/news/news.notice'	The command '/bin/grep '^s*news\\.notice' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'news.err -/var/log/news/news.err'	The command '/bin/grep '^s*news\\.err' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'news.crit -/var/log/news/news.crit'	The command '/bin/grep '^s*news\\.crit' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'mail.warning -/var/log/mail.warn'	The command '/bin/grep '^s*mail\\.warning' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'mail.info -/var/log/mail.info'	The command '/bin/grep '^s*mail\\.info' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' did not return any result
ensure logging is configured - 'mail.* - /var/log/mail'	The command '/bin/grep '^s*mail\\.\\.*' /etc/rsyslog.conf /etc/rsyslog.d/*.conf' returned :  /etc/rsyslog.d/50-default.conf:mail.* -/var/log/mail.log
Ensure outbound and established connections are configured	Executing the command '/sbin/iptables -L -v -n' failed : iptables v1.6.1: can't initialize iptables table `filter': Permission denied (you must be root)  Perhaps iptables or your kernel needs to be upgraded.
Ensure loopback traffic is configured	Executing the command '/sbin/iptables -L INPUT -v -n; /sbin/iptables -L OUTPUT -v -n' failed : iptables v1.6.1:

**COMMERCIAL-IN-CONFIDENCE**

	<p>can't initialize iptables table `filter': Permission denied (you must be root)</p> <p>Perhaps iptables or your kernel needs to be upgraded.</p> <p>iptables v1.6.1: can't initialize iptables table `filter': Permission denied (you must be root)</p> <p>Perhaps iptables or your kernel needs to be upgraded.</p>
Ensure default deny firewall policy - 'Chain OUTPUT'	<p>Executing the command '/sbin/iptables --list   /bin/grep 'Chain OUTPUT' failed :</p> <p>iptables v1.6.1: can't initialize iptables table `filter': Permission denied (you must be root)</p> <p>Perhaps iptables or your kernel needs to be upgraded.</p>
Ensure default deny firewall policy - 'Chain FORWARD'	<p>Executing the command '/sbin/iptables --list   /bin/grep 'Chain FORWARD' failed :</p> <p>iptables v1.6.1: can't initialize iptables table `filter': Permission denied (you must be root)</p> <p>Perhaps iptables or your kernel needs to be upgraded.</p>
Ensure default deny firewall policy - 'Chain INPUT'	<p>Executing the command '/sbin/iptables --list   /bin/grep 'Chain INPUT' failed :</p> <p>iptables v1.6.1: can't initialize iptables table `filter': Permission denied (you must be root)</p> <p>Perhaps iptables or your kernel needs to be upgraded.</p>
Ensure TIPC is disabled (modprobe)	<p>The command '/sbin/modprobe -n -v tipc' returned :</p> <p>insmod /lib/modules/4.15.0-36-generic/kernel/net/ipv4/udp_tunnel.ko insmod /lib/modules/4.15.0-36-generic/kernel/net/ipv6/ip6_udp_tunnel.ko insmod /lib/modules/4.15.0-36-generic/kernel/net/tipc/tipc.ko</p>
Ensure RDS is disabled (modprobe)	<p>Executing the command '/sbin/modprobe -n -v rds' failed : modprobe: FATAL: Module rds not found in directory /lib/modules/4.15.0-36-generic</p>
Ensure SCTP is disabled (modprobe)	<p>The command '/sbin/modprobe -n -v sctp' returned :</p> <p>insmod /lib/modules/4.15.0-36-generic/kernel/net/sctp/sctp.ko</p>
Ensure DCCP is disabled (modprobe)	<p>The command '/sbin/modprobe -n -v dccp' returned :</p> <p>insmod /lib/modules/4.15.0-36-generic/kernel/net/dccp/dccp.ko</p>
Ensure /etc/hosts.deny is configured	<p>The file /etc/hosts.deny does not contain <code>^\[s]*ALL</code>:</p>
Ensure /etc/hosts.allow is configured	<p>The file /etc/hosts.allow does not contain <code>^\[s]*ALL\[s]*</code>:</p>
Ensure TCP Wrappers is installed	<p>The command '/usr/bin/dpkg -s tcpd 2&gt;&amp;1' returned :</p>

## COMMERCIAL-IN-CONFIDENCE

	<p>dpkg-query: package 'tcpd' is not installed and no information is available</p> <p>Use dpkg --info (= dpkg-deb --info) to examine archive files, and dpkg --contents (= dpkg-deb --contents) to list their contents.</p>
Ensure IPv6 is disabled	<p>Non-compliant file(s): /etc/default/grub - regex '^[\s]*GRUB_CMDLINE_LINUX[\s]*=[\s]*' found - expect 'ipv6\.disable[\s]*=[\s]*1' not found in the following lines: 12: GRUB_CMDLINE_LINUX=</p>
Ensure IPv6 redirects are not accepted - 'net.ipv6.conf.default.accept_redirects' (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv6\.conf\.default\.accept_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure IPv6 redirects are not accepted - 'net.ipv6.conf.all.accept_redirects' (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv6\.conf\.all\.accept_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure IPv6 router advertisements are not accepted - 'sysctl net.ipv6.conf.default.accept_ra'	<p>The command '/sbin/sysctl net.ipv6.conf.default.accept_ra' returned :</p> <p>net.ipv6.conf.default.accept_ra = 1</p>
Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.default.accept_ra' (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv6\.conf\.default\.accept_ra[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure IPv6 router advertisements are not accepted - 'sysctl net.ipv6.conf.all.accept_ra'	<p>The command '/sbin/sysctl net.ipv6.conf.all.accept_ra' returned :</p> <p>net.ipv6.conf.all.accept_ra = 1</p>
Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.all.accept_ra' (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv6\.conf\.all\.accept_ra[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure bogus ICMP responses are ignored (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.icmp_ignore_bogus_error_responses[\s]*=[\s]*1[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure broadcast ICMP requests are ignored (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.icmp_echo_ignore_broadcasts[\s]*=[\s]*1[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure suspicious packets are logged - 'sysctl net.ipv4.conf.default.log_martians'	<p>The command '/sbin/sysctl net.ipv4.conf.default.log_martians' returned :</p> <p>net.ipv4.conf.default.log_martians = 0</p>

## COMMERCIAL-IN-CONFIDENCE

<p>Ensure suspicious packets are logged - 'net.ipv4.conf.default.log_martians' (sysctl.conf/sysctl.d)</p>	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.default\.log_martians[\s]*=[\s]*1[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
<p>Ensure suspicious packets are logged - 'sysctl net.ipv4.conf.all.log_martians'</p>	<p>The command '/sbin/sysctl net.ipv4.conf.all.log_martians' returned :</p> <p>net.ipv4.conf.all.log_martians = 0</p>
<p>Ensure suspicious packets are logged - 'net.ipv4.conf.all.log_martians' (sysctl.conf/sysctl.d)</p>	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.all\.log_martians[\s]*=[\s]*1[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
<p>Ensure secure ICMP redirects are not accepted - 'sysctl net.ipv4.conf.default.secure_redirects'</p>	<p>The command '/sbin/sysctl net.ipv4.conf.default.secure_redirects' returned :</p> <p>net.ipv4.conf.default.secure_redirects = 1</p>
<p>Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.default.secure_redirects' (sysctl.conf/sysctl.d)</p>	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.default\.secure_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
<p>Ensure secure ICMP redirects are not accepted - 'sysctl net.ipv4.conf.all.secure_redirects'</p>	<p>The command '/sbin/sysctl net.ipv4.conf.all.secure_redirects' returned :</p> <p>net.ipv4.conf.all.secure_redirects = 1</p>
<p>Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.all.secure_redirects' (sysctl.conf/sysctl.d)</p>	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.all\.secure_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
<p>Ensure ICMP redirects are not accepted - 'net.ipv4.conf.default.accept_redirects' (sysctl.conf/sysctl.d)</p>	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.default\.accept_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
<p>Ensure ICMP redirects are not accepted - 'net.ipv4.conf.all.accept_redirects' (sysctl.conf/sysctl.d)</p>	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.all\.accept_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
<p>Ensure source routed packets are not accepted - 'sysctl net.ipv4.conf.default.accept_source_route'</p>	<p>The command '/sbin/sysctl net.ipv4.conf.default.accept_source_route' returned :</p> <p>net.ipv4.conf.default.accept_source_route = 1</p>
<p>Ensure source routed packets are not accepted - 'net.ipv4.conf.default.accept_source_route' (sysctl.conf/sysctl.d)</p>	<p>The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.default\.accept_source_route[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p>

## COMMERCIAL-IN-CONFIDENCE

	fail
Ensure source routed packets are not accepted - 'net.ipv4.conf.all.accept_source_route' (sysctl.conf/sysctl.d)	The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.all\.accept_source_route[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  /usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :  fail
Ensure packet redirect sending is disabled - 'sysctl net.ipv4.conf.default.send_redirects'	The command '/sbin/sysctl net.ipv4.conf.default.send_redirects' returned :  net.ipv4.conf.default.send_redirects = 1
Ensure packet redirect sending is disabled - 'net.ipv4.conf.default.send_redirects' (sysctl.conf/sysctl.d)	The command '/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.default\.send_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  /usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :  fail
Ensure packet redirect sending is disabled - 'sysctl net.ipv4.conf.all.send_redirects'	The command '/sbin/sysctl net.ipv4.conf.all.send_redirects' returned :  net.ipv4.conf.all.send_redirects = 1
Ensure packet redirect sending is disabled - 'net.ipv4.conf.all.send_redirects' (sysctl.conf/sysctl.d)	The command '/usr/bin/grep -s -P '^[\s]*net\.ipv4\.conf\.all\.send_redirects[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  /usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :  fail
Ensure IP forwarding is disabled (sysctl.conf/sysctl.d)	The command '/bin/grep -s -P '^[\s]*net\.ipv4\.ip_forward[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  /usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :  fail
Ensure telnet client is not installed	The command '/usr/bin/dpkg -s telnet 2>&1' returned :  Package: telnet Status: install ok installed Priority: standard Section: net Installed-Size: 161 Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com> Architecture: amd64 Source: netkit-telnet Version: 0.17-41 Replaces: netstd Provides: telnet-client Depends: netbase, libc6 (>= 2.15), libstdc++6 (>= 5) Description: basic telnet client The telnet command is used for interactive communication with another host using the TELNET protocol. . For the purpose of remote login, the present client executable should be

## COMMERCIAL-IN-CONFIDENCE

	<p>depreciated in favour of an ssh-client, or in some cases with variants like telnet-ssl or Kerberized TELNET clients. The most important reason is that this implementation exchanges user name and password in clear text.</p> <p>.</p> <p>On the other hand, the present program does satisfy common use cases of network diagnostics, like protocol testing of SMTP services, so it can become handy enough.</p> <p>Original-Maintainer: Mats Erik Andersson &lt;mats.andersson@gisladisker.se&gt;</p>
Ensure rsync service is not enabled	<p>The command returned :</p> <p>enabled</p>
Ensure HTTP server is not enabled	<p>The command returned :</p> <p>enabled</p>
Ensure time synchronization is in use	
Ensure permissions on /etc/motd are configured	<p>The file /etc/motd does not exist</p> <p>/etc/motd</p>
Ensure message of the day is configured properly	<p>The file /etc/motd could not be found</p>
Ensure address space layout randomization (ASLR) is enabled (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -P '^[\s]*kernel\.randomize_va_space[\s]*=[\s]*2[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  /usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure XD/NX support is enabled	<p>The command '/bin/dmesg   /bin/grep 'NX (Execute' 2&gt;&amp;1' did not return any result</p>
Ensure core dumps are restricted - 'fs.suid_dumpable' (sysctl.conf/sysctl.d)	<p>The command '/bin/grep -s -E '^[\s]*fs\.suid_dumpable[\s]*=[\s]*0[\s]*\$' /etc/sysctl.conf /etc/sysctl.d/*  /usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure core dumps are restricted -'hard core (limits.conf/limits.d)'	<p>The command '/bin/grep -s -P '^[\s]*\*[\s]+hard[\s]+core[\s]+0[\s]*\$' /etc/security/limits.conf /etc/security/limits.d/*  /usr/bin/awk '{print} END {if (NR != 0) print pass ; else print fail}'" returned :</p> <p>fail</p>
Ensure core dumps are restricted	<p>The command '/sbin/sysctl fs.suid_dumpable' returned :</p> <p>fs.suid_dumpable = 2</p>
Ensure authentication required for single user mode	<p>The file /etc/shadow could not be found</p>
Ensure bootloader password is set - 'passwd_pbkdf2'	<p>The file /boot/grub/grub.cfg does not contain ^[\s]*password</p>
Ensure bootloader password is set - 'set superusers'	<p>The file /boot/grub/grub.cfg does not contain ^[\s]*set[\s]+superusers[\s]*=</p>
Ensure permissions on bootloader config are configured	<p>The file /boot/grub/grub.cfg with fmode owner: root group: root mode: 0444 attr: -----e--- uid: 0 gid: 0 uneven permissions :</p>

## COMMERCIAL-IN-CONFIDENCE

	<p>FALSE does not match the policy value owner: root group: root mask: 0177 uneven permissions : TRUE</p> <p>/boot/grub/grub.cfg</p>
Ensure filesystem integrity is regularly checked	<p>Executing the command '/usr/bin/crontab -u root -l   grep aide' failed :</p> <p>must be privileged to use -u</p>
Ensure AIDE is installed	<p>The command '/usr/bin/dpkg -s aide 2&gt;&amp;1' returned :</p> <p>dpkg-query: package 'aide' is not installed and no information is available</p> <p>Use dpkg --info (= dpkg-deb --info) to examine archive files, and dpkg --contents (= dpkg-deb --contents) to list their contents.</p>
Ensure GPG keys are configured	<p>The command returned :</p> <p>/etc/apt/trusted.gpg</p> <p>-----</p> <p>pub rsa4096 2014-06-13 [SC] 9FD3 B784 BC1C 6FC3 1A8A 0A1C 1655 A0AB 6857 6280 uid [ unknown] NodeSource &lt;gpg@nodesource.com&gt; sub rsa4096 2014-06-13 [E]</p> <p>pub rsa4096 2016-12-14 [SC] [expired: 2018-12-14] 2930 ADAE 8CAF 5059 EE73 BB4B 5871 2A22 91FA 4AD5 uid [ expired] MongoDB 3.6 Release Signing Key &lt;packaging@mongodb.com&gt;</p> <p>pub rsa2048 2011-08-19 [SC] [expires: 2024-06-14] 573B FD6B 3D8F BC64 1079 A6AB ABF5 BD82 7BD9 BF62 uid [ unknown] nginx signing key &lt;signing-key@nginx.com&gt;</p> <p>/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-archive.gpg</p> <p>-----</p> <p>pub rsa4096 2012-05-11 [SC] 790B C727 7767 219C 42C8 6F93 3B4F E6AC C0B2 1F32 uid [ unknown] Ubuntu Archive Automatic Signing Key (2012) &lt;ftpmaster@ubuntu.com&gt;</p> <p>/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg</p> <p>-----</p> <p>pub rsa4096 2012-05-11 [SC] 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092 uid [ unknown] Ubuntu CD Image Automatic Signing Key (2012) &lt;cdimage@ubuntu.com&gt;</p>
Ensure noexec option set on /dev/shm partition	<p>The command '/bin/mount   /bin/grep -P 'on[\s]+/dev/shm"' returned :</p> <p>tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)</p>
Ensure nodev option set on /home partition	<p>The command '/bin/mount   /bin/grep -P 'on[\s]+/home"' did not return any result</p>
Ensure noexec option set on /var/tmp partition	<p>The command '/bin/mount   /bin/grep -P 'on[\s]+/var/tmp"' did not return any result</p>
Ensure nosuid option set on /var/tmp partition	<p>The command '/bin/mount   /bin/grep -P 'on[\s]+/var/tmp"' did not return any result</p>
Ensure nodev option set on /var/tmp partition	<p>The command '/bin/mount   /bin/grep -P 'on[\s]+/var/tmp"' did not return any result</p>



## COMMERCIAL-IN-CONFIDENCE

Ensure nosuid option set on /tmp partition	The command '/bin/mount   /bin/grep -P 'on[\s]+/tmp"' did not return any result
Ensure nodev option set on /tmp partition	The command '/bin/mount   /bin/grep -P 'on[\s]+/tmp"' did not return any result
Ensure mounting of udf filesystems is disabled (modprobe)	The command '/sbin/modprobe -n -v udf' returned : insmod /lib/modules/4.15.0-36-generic/kernel/lib/crc-itu-t.ko insmod /lib/modules/4.15.0-36-generic/kernel/fs/udf/udf.ko
Ensure mounting of hfsplus filesystems is disabled (hfsplus)	Executing the command '/sbin/modprobe -n -v hfsplus' failed : modprobe: FATAL: Module hfsplus not found in directory /lib/modules/4.15.0-36-generic
Ensure mounting of hfs filesystems is disabled (modprobe)	Executing the command '/sbin/modprobe -n -v hfs' failed : modprobe: FATAL: Module hfs not found in directory /lib/modules/4.15.0-36-generic
Ensure mounting of jffs2 filesystems is disabled (modprobe)	Executing the command '/sbin/modprobe -n -v jffs2' failed : modprobe: FATAL: Module jffs2 not found in directory /lib/modules/4.15.0-36-generic
Ensure mounting of freevxfs filesystems is disabled (modprobe)	Executing the command '/sbin/modprobe -n -v freevxfs' failed : modprobe: FATAL: Module freevxfs not found in directory /lib/modules/4.15.0-36-generic
Ensure mounting of cramfs filesystems is disabled (modprobe)	Executing the command '/sbin/modprobe -n -v cramfs' failed : modprobe: FATAL: Module cramfs not found in directory /lib/modules/4.15.0-36-generic

**Table 3 - UNIX failed compliance onvps544591 (54.38.214.253)**

## Appendix C - Findings Definitions

BSI Cybersecurity and Information Resilience have developed a method for evaluating vulnerabilities and presenting the results in a way which enables clients to easily assess the risks they pose to the organisation.

### C.1. Risk Ratings

Each finding is categories by its "Seriousness" and "Likelihood". The overall risk rating is calculated as a multiple of the two values.

$$\text{Overall risk} = \text{Seriousness} \times \text{Likelihood}$$

Below are guidance on rating definitions; exact ratings may depend on particular environment.

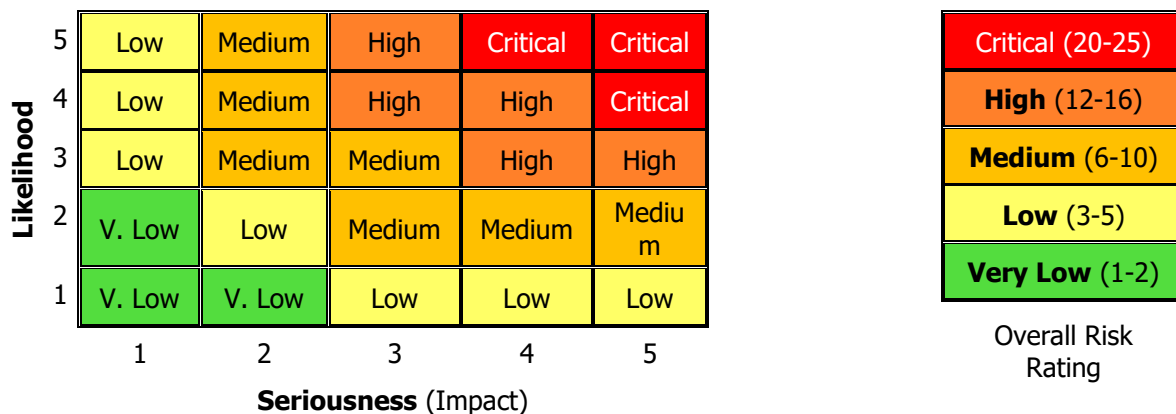
#### Seriousness (Impact)

- 5** - Remotely gaining administrative access;
- 4** - Remote privilege escalation or unauthorised read/write access;
- 3** - Local privilege escalation or unauthorised read-only access to data;
- 2** - Sensitive information disclosure. Minor security configuration weakness;
- 1** - Minor non-sensitive information disclosure.

#### Likelihood (exploitability)

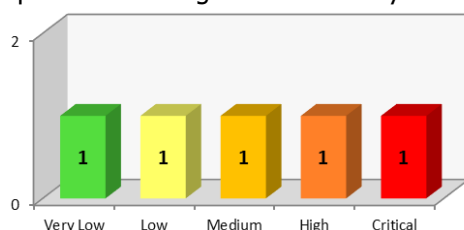
- 5** - Trivial to exploit by unskilled person;
- 4** - Require exploit code or tool which was in the public domain, or easy to exploit with some knowledge;
- 3** - Require some exploit code development or effort to exploit, or require specific knowledge/skill;
- 2** - Attacker may require specific access;
- 1** - Theoretical vulnerability where there is no known exploit code and/or would require a lot of resources to exploit.

Rating may also take in to account existing defences which may restrict the exploitability.



### C.2. Executive Summary

The executive summary provides a number of graphical representations as to the most common root cause of the vulnerabilities identified. A summary of the number of different root cause categories are summarised in a graph in the management summary.



In addition, all findings are plotted onto a graph so that the severity of the vulnerabilities identified can easily be visualised. This enables the client to concentrate their efforts for resolution in specific areas



The pie chart depicts the most common root causes of the vulnerabilities identified.

**C.2.1. Root Causes**

The root causes for infrastructure tests include:

- ❖ Configuration
- ❖ Encryption
- ❖ Human Factor
- ❖ Network Design
- ❖ Password Policy
- ❖ Patching
- ❖ Web Development

The root causes for application tests include:

- ❖ Authentication
- ❖ Client Side Controls
- ❖ Configuration
- ❖ Default Content
- ❖ Design Error
- ❖ Encryption
- ❖ Input Validation
- ❖ Logic Error
- ❖ Password Policy
- ❖ Session Control

**C.3. Findings Box**

The table below provides a key to understand the findings description.

<b>Finding No. X</b>	Systems Affected	List of devices which are vulnerable. This will either take the form of IP addresses (DNS names) or URLs.
	Finding	An overview of the vulnerability identified.
	CVE number	Where possible, references will be made to a common reference identifier such as CVE or CWE. These references to external sources allow clients to find out additional details regarding the vulnerability and how to mitigate it.
	Root Cause	Each finding will be categorised as to the perceived root cause. Further details are discussed in the section below.
	Seriousness (Impact)	Impact if the vulnerability is successfully exploited. Rated from 5 (serious) to 1(not serious). <div style="display: flex; align-items: center; justify-content: center;"> <div style="margin-right: 10px;">                     5 - <span style="color: green;">■</span> <span style="color: yellow;">■</span> <span style="color: orange;">■</span> <span style="color: red;">■</span>                      4 - <span style="color: green;">■</span> <span style="color: yellow;">■</span> <span style="color: orange;">■</span> <span style="color: red;">■</span>                      3 - <span style="color: green;">■</span> <span style="color: yellow;">■</span> <span style="color: orange;">■</span> <span style="color: red;">■</span>                      2 - <span style="color: green;">■</span> <span style="color: yellow;">■</span> <span style="color: orange;">■</span> <span style="color: red;">■</span>                      1 - <span style="color: green;">■</span> <span style="color: yellow;">■</span> <span style="color: orange;">■</span> <span style="color: red;">■</span> </div> <div style="margin-left: 10px;">                     (visual representation)                 </div> </div>
	Likelihood	How easy is the vulnerability to exploit? Ratings from 5 (easy) to 1 (difficult).
	Overall Risk rating	The overall risk rating takes into account the seriousness of the issue, the likelihood of the vulnerability being exploited, as well as other factors that could impact the overall risk.

Note: It should be noted that the definitions defined above for the seriousness and likelihood ratings are only guidelines.