Logo

Description automatically generated

***Protecting our Information***

**VIRGIN MEDIA O2**

**Server Configuration Standard Exception**

**On-Premise RHEL 8.4 Build Development**

CIRCULATION LIST *(individual and role)*

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Business Unit or company name** |
| Samydurai Hariraman | Build Manager | TCS |
| Peter Chung |  | Fraud & Security |
| Seth Yates | Senior Systems Administrator | TCS |
| Fai Tao | Senior Systems Administrator | TCS |
| Julian Jeffery | Head of Policy & CR | Fraud & Security |
| Joy Turner | Security Risk & Reporting Manager | Fraud & Security |

ALL RIGHTS RESERVED

This is an unpublished work. No part of this document may be copied, photocopied, reproduced, translated or reduced to any electronic or machine-readable form without the prior permission of Telefónica UK Limited.

What Is Risk

* For the purposes of the document, risk is the probability that a particular security threat, if exploited, will trigger or initiate a potential impact to the Telefónica UKbusiness which could lead to financial loss or impact to brand name.

**Risk = Threat x Ease of Exploitation x Likelihood of Exploitation x Impact**

* In breaking down the security risk in this way, the security requirements and the non compliance implications are better evaluated, prioritised and managed when estimating overall project requirement and the potential impact of non compliancy with any of the security requirements.

Explanation of Hardening risk rating symbols

|  |  |
| --- | --- |
| **Severity Of Risk** | **Hardening Risk Classification** |
| High 💣💣💣 | * Of greatest concern, must be implemented. The identified hardening recommendation is considered to have a high likelihood of exploitation, easy to exploit, far-reaching in scope, has the potential of a significant impact if exploited or is not being resolved by mitigating controls. |
| Medium 💣💣 | * Of concern, addresses an attack or issue that should be mitigated by implementing the recommendation. The recommendation is considered to have a moderate likelihood of exploitation, to have a moderate impact if exploited, or to be partially resolved by compensating controls. |
| Low 💣 | * Of little overall security concern, but of benefit to implement. Hardening recommendation is considered to be very unlikely to lead to a compromise, to have a low impact if exploitation was to occur, or to be acceptably controlled by existing configuration safeguards and compensating controls. |

# 1. INTRODUCTION

Telefónica UK strives to ensure that its systems and services comply with the industry standards when protecting customer’s data and to that end, Telefónica UK has introduced various security hardening standards across its business to ensure that all systems have a minimum security baseline that can be reviewed for compliance and gives the business owner a level of confidence that their system has an acceptable security posture. Hardening standards form the basis of a security configuration policy that removes all know default configuration issues and allows the system to be protected against known vulnerabilities that can be exploited by a malicious user. All systems that can not comply with the appropriate security hardening standard must apply for a security hardening exception to the requirement that must be approved by the appropriate security team and business owner or senior manager taking into account the provisions set out in the Telefónica Europe Risk Management Policy on acceptance of risk and individuals delegated authority limits.

This documents aim is to ensure that all Telefónica UK systems have a auditable security posture which is applied across the **RHEL 8 Standard Build** platform.

1.1 This document relates to the **RHEL 8 Standard Build** platform only.

1.2 This document is provided to explain the potential risks caused by this exception to the Telefónica UK security hardening standard being accepted, the mitigation in place to manage this risk and the recommendation that the risk be accepted.

**Important Note:** this exception will cover the servers relating to the **RHEL 8 Standard Build** platform and all non compliances must have a justifiable business reason and assigned risk level for all non compliances with the security hardening standard.

# 2. REASONS FOR EXCEPTION REQUEST

2.1 It is requested that a **RHEL 8 Standard Build platform** business exception to the “**CIS Red Hat Enterprise Linux 8 Benchmark v1.0.1”** is granted against all **RHEL 8.4.** Any additional exception will require an amendment to this document and further approval for the system exception.

2.2 All exceptions listed in this document will reduce functionality considerably; the majority of which pose low threat to corporate data being compromised. All exceptions will however be reviewed on a yearly basis.

# 3. RISK ASSESSMENT

3.1 **The Risk** - Before requesting this exception a risk analysis has been conducted to see what compensating controls are in place which would mitigate this risk. A list of non compliances can be viewed in the Appendix A.

3.2 **Mitigation** – The following has been put in place as business mitigation overview and specific controls with business justification can be viewed in Appendix A

* All exceptions have compensating controls in place that will mitigate any potential risk. These will also be reviewed yearly.

3.3 **Outcome** – The **RHEL 8.4 Standard Build** project team believe that there are sufficient mitigating controls in place (where technically possible) which act to prevent any potential risk of corporate data being compromised.

3.4 F&S have no objection to this exception being granted.

3.5 **Exception Risk Level** = **Low**

3.6 **Risk Level Justification**

The risk assignment has been assessed as low due to the average risk level assigned to all risks. Amount of non compliances that have been identified that need an exception until further investigation and testing can be arranged

4. RISK AUTHORISATION

4.1 The Telefónica UK Security Hardening Standard exceptions process requires that exceptions to any security standards are authorised at the appropriate level of the business. This document is therefore submitted to Peter Chungto evaluate this request and advise F&S if they are prepared to accept the risk of not conforming to the CIS Security Hardening Standard on this case.

4.2 This risk has been placed on the Technology Risk Register and will be reviewed within 12 months, and then on a continual 12 month basis, to ensure that the exception is still appropriate and approved by **Sean Yeates**. Any additional system non compliance will require amendment to this exception document raised for that service.

4.3 **Risk Acceptance**

**Exception Start Date: 3/Mar/2022**

**Exception Raised By: Seth Yates / Samydurai**

**Exception Approved By: Sean Yeates**

**Exception Expiry Date: 2 / Mar /2023**

Detailed information can be found below documents

CIS Red Hat Enterprise Linux 8 Benchmark v1.0.1

****

**Appendix A**

**List of Security Hardening Exceptions**

| **CIS Ref No** | **CIS Requirement** | **Description** | **Business Justification** | **Risk level** |
| --- | --- | --- | --- | --- |
| 1.4.2 | [Ensure filesystem integrity is regularly checked](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d232) | Description:  Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.  Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion. | False positive.  The required cron job exists.However CIS is not detecting and failing. | Low risk |
| |  |  | | --- | --- | |  | [3.4.3.4](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d301) | | [Ensure nftables loopback traffic is configured](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d301) | Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network  Loopback traffic is generated between processes on a machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure. | The firewalld service is enabled and manages nftables.  We can add a rule to firewalld for loopback traffic, but this doesn't get a pass in CIS. | Low risk |
| [3.4.3.6](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d303) | [Ensure nftables default deny firewall policy](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d303) | Description:  Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.  There are two policies: accept (Default) and drop. If the policy is set to accept , the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.  It is easier to white list acceptable usage than to black list unacceptable usage. | The firewalld service is enabled and manages nftables.  We can change the "target" for firewalld from "default" to "DROP", which adds blocking of ping, but this doesn't get a pass in CIS. | Low risk |
| |  |  | | --- | --- | |  | [3.4.3.7](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d304) | | [Ensure nftables service is enabled](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d304) | Description:  The nftables service allows for the loading of nftables rulesets during boot, or starting of the nftables service  The nftables service restores the nftables rules from the rules files referenced in the /etc/sysconfig/nftables.conf file durring boot or the starting of the nftables service | The firewalld service is enabled and manages nftables. | Low risk |
| |  |  | | --- | --- | |  | [3.4.3.8](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d305) | | [Ensure nftables rules are permanent](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.4\2022%20-Mar%20Review\dmmlw-rhel84-002-report-20220203T111610Z\dmmlw-rhel84-002-report-20220203T111610Z.html#detail-w107aad407d305) | Description:  nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.  The nftables service reads the /etc/sysconfig/nftables.conf file for a nftables file or files to include in the nftables ruleset.  A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.  Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot. | The firewalld service is enabled and manages nftables. | Low risk |
| 4.2.1.5 | Ensure rsyslog is configured to send logs to a remote log host | The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing administrative overhead. | False positive  Initial builds have a templated config for this, but require additional information from the Arcsight team on the particular log host is used to finalise. | Low risk |
| 4.2.3 | Ensure permissions on all logfiles are configured | Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well. | The main system log (/var/adm/messages) needs to be readable by all so BMC Patrol can perform all required monitoring.  A few other log files are also readable by regular users. These file don’t contain sensitive information and may be useful for regular users to have read access. | Low risk |
| 5.5.2 | [Ensure system accounts are secured](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.2\cnmlw-rhel82-001-report-20201127T175625Z.HTML#detail-w107aad287d329) | There are a number of accounts provided with Red Hat 7 that are used to manage applications and are not intended to provide an interactive shell. | The following user accounts are the cause of the failure: metron, patrol, patrolcon, oracle, and qualys. All of these require login access and the UID number (below 1000 is considered system accounts) are dictated by the teams which use these accounts.  Metron = 120  Patrol = 124  Patrolcon = 125  Oracle = 200  Qualys = 123  These UIDs are decided by the particular teams in their documentation. They’re not system accounts as such, ie. not part of a standard operating system and do require interactive shell to be useful. | Low risk |
| 6.2.7 | [Ensure users' home directories permissions are 750 or more restrictive](file:///C:\Users\hariras1\Desktop\Build%20Review\RHEL%208.2\cnmlw-rhel82-001-report-20201127T175625Z.HTML#detail-w107aad287d366) | Description:  While the system administrator can establish secure permissions for users' home directories, the users can easily override these.  Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.  Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy. | Patrol prerequisities required same home directory (/opt/BMC/PATROL) and group write permission set for Patrol and patrolcon users.  Exception required for enabling group write permission. |  |
| 6.2.8 | Ensure users own their home directories | The user home directory is space defined for the particular user to set local environment variables and to store personal files. | As a Patrol prerequisities, Patrol and Patrolcon users sharing same  home directory(/opt/BMC/PATROL) . Exception required as two users sharing same home directory. | Low risk |