****

***Protecting our Information***

**Telefónica UK**

**Server Configuration Standard Exception**

**ITPC RHEL 8.3 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This is an unpublished work.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 v1.0.0.1”** is granted against all **RHEL 8.3.** 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 8.3 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: 12/Aug/2021**

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

**Exception Approved By: Sean Yeates**

**Exception Expiry Date:13/08/2022**

Detailed information can be found below documents

CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0.1



**Appendix A**

**List of Security Hardening Exceptions**

| **CIS Ref No** | **CIS Requirement** | **Description** | **Business Justification** | **Risk level** |
| --- | --- | --- | --- | --- |
| 3.4.2.1 | [Ensure firewalld service is enabled and running](file:///C:\Users\hariras1\Desktop\Build%20Review\ITPC\Jan%202021\carl-test-vm.itpc.uk.pri.o2.com-report-20210122T170633Z\carl-test-vm.itpc.uk.pri.o2.com-report-20210122T170633Z.html#detail-w107aad287d232) | Ensure that the firewalld service is enabled to protect your system  firewalld (Dynamic Firewall Manager) tool provides a dynamically managed firewall. The tool enables network/firewall zones to define the trust level of network connections and/or interfaces. It has support both for IPv4 and IPv6 firewall settings. Also, it supports Ethernet bridges and allow you to separate between runtime and permanent configuration options. Finally, it supports an interface for services or applications to add firewall rules directly | Host-based firewalls aren’t to be used with ITPC. | Low Risk |
| 3.4.3.7 | Ensure nftables service is enabled | 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 | Host-based firewalls aren’t to be used with ITPC. | 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.  It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected. | 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 |
| 6.2.14 | [Ensure all groups in /etc/passwd exist in /etc/group](file:///C:\Users\hariras1\Desktop\Build%20Review\ITPC\Jan%202021\carl-test-vm.itpc.uk.pri.o2.com-report-20210122T170633Z\carl-test-vm.itpc.uk.pri.o2.com-report-20210122T170633Z.html#detail-w107aad287d353) | Description:  Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group .  Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed. | False positive. All groups exist in /etc/group. Perhaps this is failing due to no additional users/groups added at this point | Low risk |
| 6.2.20 | Ensure all users' home directories exist | Description:  Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.  If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set. | Failed.  Looks like the ‘fail’ status is due to no users being present, so nothing under /home. Creating a dummy account to satisfy CIS seems counter-productive from a security perspective. | Low risk |