Logo

Description automatically generated

***Protecting our Information***

**VIRGIN MEDIA O2**

**Server Configuration Standard Exception**

**On-Premise RHEL 9.0 Build Development**

CIRCULATION LIST *(individual and role)*

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Business Unit or company name** |
| Samydurai Hariraman | Build Manager | TCS |
| Peter Chung | IT Secuity | Fraud & Security |
| Seth Yates | Senior Systems Administrator | TCS |
| Fai Tao | Senior Systems Administrator | TCS |
| Harry Clarke | Policy & CR | Fraud & Security |
| Bathany Jackman | 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This is an unpublished work.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 VMO2 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 VMO2business 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

VMO2 strives to ensure that its systems and services comply with the industry standards when protecting customer’s data and to that end, VMO2 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 VMO2 systems have a auditable security posture which is applied across the **RHEL 9 Standard Build** platform.

1.1 This document relates to the **RHEL 9 Standard Build** platform only.

1.2 This document is provided to explain the potential risks caused by this exception to the VMO2 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 9 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 9 Standard Build platform** business exception to the “**CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0”** is granted against all **RHEL 9.0.** 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 9.0 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 VMO2 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: 22/12/2022**

**Exception Raised By: Seth Yates**

**Exception Approved By: Sean Yeates**

**Exception Expiry Date: 22/12/2023**

Detailed information can be found below documents

CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0 - Level 2

****

**Appendix A**

**List of Security Hardening Exceptions**

| **CIS Ref No** | **CIS Requirement** | **Description** | **Business Justification** | **Risk level** |
| --- | --- | --- | --- | --- |
| 1.1.4.1 | Ensure separate partition exists for /var/tmp | The /var/tmp directory is a world-writable directory used for temporary storage by all users and some applications. Temporary files residing in /var/tmp are to be preserved between reboots. | Not part of standard disk layout.  /var/tmp is bound to /tmp and so occupies the same disk space as /tmp rather than the /var partition. | Low risk |
| |  |  | | --- | --- | |  | 1.1.6.1 | | Ensure separate partition exists for /var/log/audit | The auditing daemon, auditd , stores log data in the /var/log/audit directory. | Not part of standard disk layout.  This is part of the /var/log partition and the local audit logs are rotated frequently to avoid filling this partition. | Low risk |
| 3.3.7 | Ensure Reverse Path Filtering is enabled | Description:  Setting net.ipv4.conf.all.rp\_filter and net.ipv4.conf.default.rp\_filter to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if log\_martians is set).  Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing. | False positive.  The kernel parameters are set, but the benchmark cannot properly detect them. CIS support are investigating. | Low risk |
| |  |  | | --- | --- | |  | 3.4.2.4 | | Ensure host based firewall loopback traffic is configured | Description:  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 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. | Loopback traffic is already blocked from the external interface with the current firewall configuration.  The requirements for this refinement are unclear as benchmark is still in development. When clearer this can be implemented. | Low risk |
| |  |  | | --- | --- | |  | 4.1.2.2 | | Ensure audit logs are not automatically deleted | Description:  The max\_log\_file\_action setting determines how to handle the audit log file reaching the max file size. A value of keep\_logs will rotate the logs but never delete old logs.  In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history. | This would quickly fill the /var/log partition or would require a lot of additional disk space for every server.  The audit logs should be maintained in Arcsight to be of any use. | Low risk |
| 4.1.2.3 | Ensure system is disabled when audit logs are full | Description:  The auditd daemon can be configured to halt the system when the audit logs are full.  The admin\_space\_left\_action parameter tells the system what action to take when the system has detected that it is low on disk space. Valid values are ignore, syslog, suspend, single, and halt.  ignore , the audit daemon does nothing  Syslog , the audit daemon will issue a warning to syslog  Suspend , the audit daemon will stop writing records to the disk  single , the audit daemon will put the computer system in single user mode  halt , the audit daemon will shut down the system  In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability. | This would cause all servers to shutdown soon after being put into use, unless a lot of additional disk space was given.  This would be service affecting. | Low risk |
| 4.2.3 | Ensure all logfiles have appropriate permissions and ownership | Description:  Log files contain information from many services on the local system, or in the event of a centralized log server, others system’s logs as well. In general log files are found in /var/log/ , although application can be configured to store logs elsewhere. Should your application store its logs in another location, ensure to run the same test on that location.  It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them. | 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 |
| 5.3.4 | Ensure users must provide password for escalation | Description:  The operating system must be configured so that users must provide a password for privilege escalation.  Without re-authentication, users may access resources or perform tasks for which they do not have authorization.  When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate. | Some application/service users require password-less sudo access to function.  Accounts:  blpa  bmcadmin  qualys |  |
| 5.6.1.4 | Ensure inactive password lock is 30 days or less | Description:  User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.  Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies. | Failing on the root account. This account shouldn’t be locked | Low risk |
| 5.6.2 | Ensure system accounts are secured | Description:  There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.  It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the nologin shell. This prevents the account from potentially being used to run any commands. | 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 |
| 6.2.11 | Ensure local interactive users own their home directories | Description:  The user home directory is space defined for the particular user to set local environment variables and to store personal files.  Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory. | 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 |
| 6.2.12 | Ensure local interactive user home directories are mode 750 or more restrictive | 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. | 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. | Low risk |