Reward Gateway Patch Management Policy

Classification – Confidential

10 March 2018 – Version 3.0

RewardGateway
the employee engagement people

265 Tottenham Court Road
London
W1T 7RQ
UK

Table of contents

Document purpose

This document sets out the patching policy which is applied throughout all of Reward Gateway's systems. This includes all information systems in our office network and those hosted by **Amazon Web Services EMEA SARL/AWS .** Patch management of our systems will reduce the risk of malware attacks and exposure of company information.

While patches could be received through different channels in Reward Gateway these are usually streamed as updates from the official OS repository. In this document the word "patch" and "update" may substitute one another.

General approach

Reward Gateway treats security as its number one priority. As part of this, proactive monitoring and review of the wider security environment has been adopted. Additionally, ensuring that all services are up-to-date is part of our ongoing PCI DSS compliance requirements.

Security lists

Reward Gateway monitor the following security lists for alerts:

- https://lwn.net/Alerts/CentOS/
- https://github.com/Roave/SecurityAdvisories

Whilst other lists are available, we accept that it is appropriate to wait for vendor updates as opposed to apply unverified changes.

Cloud computing environment details

Within AWS environment, there are several layers of software. The list below is a guide to each layer:

Layer	Description
Hypervisor	Reward Gateway operate virtual machines (Instances) on top of a hypervisor layer managed by AWS.
Networks (VPC)	Reward Gateway operate virtual machines and other AWS managed services - like databases - on top of a network layer (virtual private cloud or VPC) managed by Reward Gateway

Operating system	All instances managed by Reward Gateway are running CentOS 7. This is a Long Term Support (LTS) release that continues to receive security updates until 2024 [1]. The instances are deployed following the paradigm of immutable infrastructure so when a OS updates comes in, a new instance will be deployed with a new Amazon Machine Image (AMI) updated to the last OS version and deployed on Production after being tested on Staging. A Master Amazon machine Image (AMI) will be created using our automated build system every time that a new update comes in [1] https://wiki.centos.org/About/Product
Kubernetes Cluster	A kubernetes cluster is deployed in order to orchestrate the function of the containers serving our applications. The cluster has two main layers: Control plane and worker nodes. The control plane of the cluster is provided and managed by Amazon EKS (Managed kubernetes service). And deployed using Terraform. The worker nodes are instances based on our AMI. Those instances are bootstrapped with the needed software (docker and kubelet) in order to be part of the cluster. They are deployed using Terraform and Puppet.
Application services	Reward Gateway run several mission-critical software pieces in the form of containers running on top of the Kubernetes Cluster, such as the web server software. All software at this layer is configured through Terraform and Puppet maintained in a version control system.
Third party libraries	Reward Gateway is a large application and relies on several third-party libraries. This is handled through Composer, a package management tool.
Application	Reward Gateway itself is written in PHP and is version controlled.

Office environment

This policy also applies to all software and servers operated by Reward Gateway in its office premises which are as follows:

Layer	Description

Workstations – laptops & desktops	This includes each employee workstation, which may run Linux, MAC OS X, or Windows operating systems.
On-premises servers	Servers located in the server room in our office. There are no critical servers operating in the office but patches still need to be applied.
Network equipment	Network equipment includes firewalls, switches, Wi-Fi devices, network printers, and PBX systems.

Cloud computing environment

This section describes the main points of Reward Gateway's AWS environment hosting the Reward Gateway application. It covers:

- Monitoring of various components
- The Change Management process
- Service Level Agreements

Monitoring

One of the core principles of patch management is to understand when patches are available and the life cycle of the deployed software.

Hypervisor

This layer is managed by AWS. Patches are reviewed and applied in accordance with AWS Standard Operating Procedures.

Network Layer (VPC)

This layer is managed by Reward Gateway as part of the infrastructure deployed on AWS.

Amazon Machine Image (AMI)

This layer includes all applications and files that provide the basic operating system (OS) functionalities and cannot be removed from the system. The OS is a Long Term Support (LTS) release which is deployed on all Instances in the fleet. Upgrades to newer LTS versions, should be reviewed as and when they are available.

Monitoring of available OS patches is performed daily by visiting Centos security lists and through notifications sent by Tenable Cloud to the DevOps team whenever the official package repository gets updated. DevOps team is responsible to evaluation each update as part of the process and determine its significance. For this purpose the vulnerability CVSS value is always taken into an account.

Kubernetes Cluster

This layer is a mixed environment formed of:

- A Control Plane: The DevOps team will be subscribed to the updates and notified when a new update is available.
- Worker nodes: The worker nodes are regular virtual machines or instances deployed as part of the cluster. The monitoring of patches and updates will be the same we've put in place for OS (section above)

Application Services

This group represents the core applications used to support Reward Gateway's website, for example, the database, web server, PHP interpreter etc. installed on top of the OS. These components may have exposure to the internet.

Tenable Cloud is used to monitor these packages. The tool compares the currently installed software to the latest available, specifically that in the security channels. Results from this are sent monthly to the DevOps team for evaluation of their significance.

Third-party Dependencies

Third-party dependencies are controlled through language specific package management tools, e.g. NPM or Composer.

The dependencies are checked using Black Duck, a tool made by Synopsys, which checks for known vulnerabilities and licencing issues. Results of these checks are visible in the Continuous Integration artifacts.

For PHP projects using Composer, Roave LLC's Security Advisory repository is also used during development and prevents known vulnerable packages from being adopted.

Application Layer

Reward Gateway has commissioned the following application layer scans:

- Tenable Cloud Scanner – weekly
- Tenable Cloud Scanner ASV - monthly
- Consultant-lead manual Penetration Tests – annually

Results from these scans are reviewed and treated in accordance with the our Vulnerability Management Policy, taking into account regulatory requirements, eg. PCI DSS .

Monitoring Table

Layer	Monitoring Tool	Who	When
Hypervisor	• AWS Internal	AWS	As per AWS Shared Responsibility Model
Network Layer (VPC)			
Amazon Machine Image	• Tenable Cloud • Security Lists	DevOps	Daily
Kubernetes	• AWS tools	DevOps	As per AWS Shared Responsibility Model
Application Services	• Tenable Cloud • Security Lists	DevOps	Daily
Third-party Dependencies	• SensioLab Scanner • Black Duck	DevOps	Daily
Application Layer	• Tenable Cloud • ASV scan	Security Team	Monthly

Change management process

After a patch has been flagged as missing, it must be applied to the environment. This section outlines the approach to be adopted and is governed by Reward Gateway's Change Management policy. Patching of production systems is never treated as a **standard** change and it is intentionally omitted in this document.

Hypervisor

In line with AWS Standard Operating Procedures, Reward Gateway will receive notification of the need to apply a patch at this layer. AWS is expected to provide a detailed report on the details of the proposed change that would allow assessment according to Reward Gateway Change Management policy. This would be classed as either **emergency** or **significant** change.

Network Layer

There is no need to manage Patches or updates on this layer apart from the elements that provides NAT outbound connections from our internal networks to any External Host. This updates will be treated as any Operating System update. (See section above)

Operating system

After DevOps evaluation has taken place to determine the significance of the patch it must be applied according to the Change Management policy. Updates that provide additional features to the base OS applications and do not have an impact on security should be classified as **significant** and implemented according to the plan. Updates in this group must be tested on Staging before deployment on Production.

Full change at this layer (e.g. complete OS migration to a newer LTS version) would require intensive planning and verification stages. A plan would be developed in accordance with the Change Management policy at this level.

Kubernetes Clusters

Control plane: After receiving the information about the new version available using the monitoring tools described previously, the DevOps team will proceed to update the control plane version using Terraform.

Kubernetes workers: Same Process applies for OS and Kubernetes workers (See section above)

Application services

Changes at this layer are either likely to be **emergency** changes (e.g. zero-day vulnerability in a web-facing service) or **significant** changes (e.g. privilege escalation of a local user). The process is as follows in both cases:

1. Update performed to Staging environment configuration and reviewed by either Principal Software Engineer or Chief Technical Architect.
2. Change deployed to Staging environment and validated.
3. Update performed to Production environment configuration.
4. Change deployed to Production environment on a rolling basis and validated.

During the period that the change is being applied to the Production environment, standard monitoring is in place to highlight any issues. If a problem is detected, the following process should be followed:

1. Upgraded machines removed from Production environment – this is configured in an N+1 fashion.
2. Rollback plan executed – may include failover to the disaster recovery environment.
3. Review of logs on the isolated machines and an alternative strategy adopted.

All activity should be recorded against the ticket in both failure and success outcomes.

Once the Production environment on the main site (Ireland Region (eu-west-1) has been upgraded, the last step is to deploy the change to the disaster recovery environment. (eu-central-1)

Third party libraries

Similar to the application services, if a vulnerability is identified in a third party library, an assessment should be taken on whether an **emergency** or **significant** change should be made. The key consideration here is when the change is applied:

- A **significant** change would go live as part of the weekly release cycle.
- An **emergency** change would be deployed within 4 hours.

Please refer to the Release Management document for details of how these are managed.

Service Level Agreements

The table below shows the target application times for patches at each layer:

Layer	Emergency	Significant
Hypervisor	*Refer to AWS Standard Operating Procedures*	
Networks	1 day	4 weeks
Operating System	1 day	4 weeks
Application Services	1 day	1 week
Third Party Libraries	4 hours	1 week
Application	4 hours	1 week

Office environment

Monitoring

Workstations and servers

Reward Gateway uses software called JAMF (Panorama9 used on older laptops) for monitoring the patch level on all workstations and servers in our offices. The program uses an agent software which must be installed on all Mac, Windows, and Linux workstations and servers, which will provide monitoring of the installed software and versions.

Where a major vulnerability is discovered, a patch report can be generated so IT can ensure the specific patch has been applied to all relevant machines.

Network equipment

We use various vendors for our office infrastructure. The monitoring relies on vendor security advisories so we subscribed to the vendors listed below:

- Cisco – switches
- Meraki – WiFi AP
- SonicWall – firewalls

- Mikrotik – firewalls
- HP – switches

Change management

Workstations and servers

The Panorama9 agent can be configured to apply patches and updates on workstations and servers either automatically or through a manual push operation. Most patches are provisioned automatically, except for major system updates which should be tested before being rolled out company-wide. Reward Gateway Chromebooks are automatically updated. However, there is a selection of Chromebooks which Beta updates are applied to first. This is to test for any issues before being rolled out company-wide.

Network equipment

Network equipment is patched manually according to the Operational Level Agreements (OLA) in the next section.

Operational Level Agreements

The table below shows target times for patches on each component in the office environment. These systems do not support any customer facing service directly so it is referred to as an OLA which supports SLAs in achieving their goal.

Layer	Emergency	Standard
Workstations	2 days	Automatic
On-premises servers	1 week	Planned
Network equipment	1 day	Planned

Revision history

Rev	Date	Author	Description	Approved	Date
1.0	24.03.2014	Will Tracz	Initial draft.	Richard Hurd-Wood	30.03.2014
2.0	10.08.2015	Ivan Dichev	Merge of office policy with the one for The Bunker. Formatting update.	Richard Hurd-Wood	20.08.2015
2.1	11.04.2016	Will Tracz	Change to security advisory source.	Richard Hurd-Wood	23.05.16
2.2	27.02.2016	Asen Varsanov	Update Web Application Scanner.	Will Tracz	01.03.17
2.3	01.03.2017	Liam Jones	Rebrand and general clean.	Will Tracz	03.03.2017
2.4	12.05.2017	Ivan Dichev	Clarify patching timescales.	Will Tracz	22.05.2017
2.5	26.11.2018	Asen Varsanov	Update and review.	Will Tracz	26.11.2018
3.0	16.01.2019	Miguel Arranz Sanjaya Palinda	• (MA) Replaced any mention to the bunker with AWS. Network and Hypervisor now are two different layers • (SP) Replaced mention to Panorama9 and legacy tools with JAMF Pro	Will Tracz	18.03.2019