AccessReal

Security Patch Update Specification

Version 1.0

i-Sprint
Trust without Boundaries

Table of Contents

1 Overview

1.1 Purpose

The system or software that is lack of security patch in time may suffer from attacks, may invite unauthorized access or the system stops working. If worst comes to worst, it may cause information leakage or business stops. Therefore, lack of security patch is worse than the network attacks. This document lists the security patch flow to make sure the AccessReal system can deploy security patch in time for security purpose.

See the security patch flow in this document to deploy the desired patches for effective deployment.

The security patch flow targets:

- To check the patch update of the various OS, app, hardware system regularly.
- To clarify the requirements and carry out the patch installation.
- To display the security patch update flow and its related tables.
- To list the staff tasks and duties for the security patch flow.

1.2 Target

This document is used for the server, database, and others of the AccessReal production environment that deployed at AliCloud.

1.3 Premise and Deployment Timing

To fulfill/prepare the premises listed below for successful security patch implementation.

i. The patch that is recommended by the system admin can be obtained via the secured channels.
ii. The security vulnerabilities caused by the OS or the software configurations can be fixed by modifying the configurations of the current environment or adjusting its functionality.
iii. The security patch is released by the vendor and is obtained via the current secured channels.

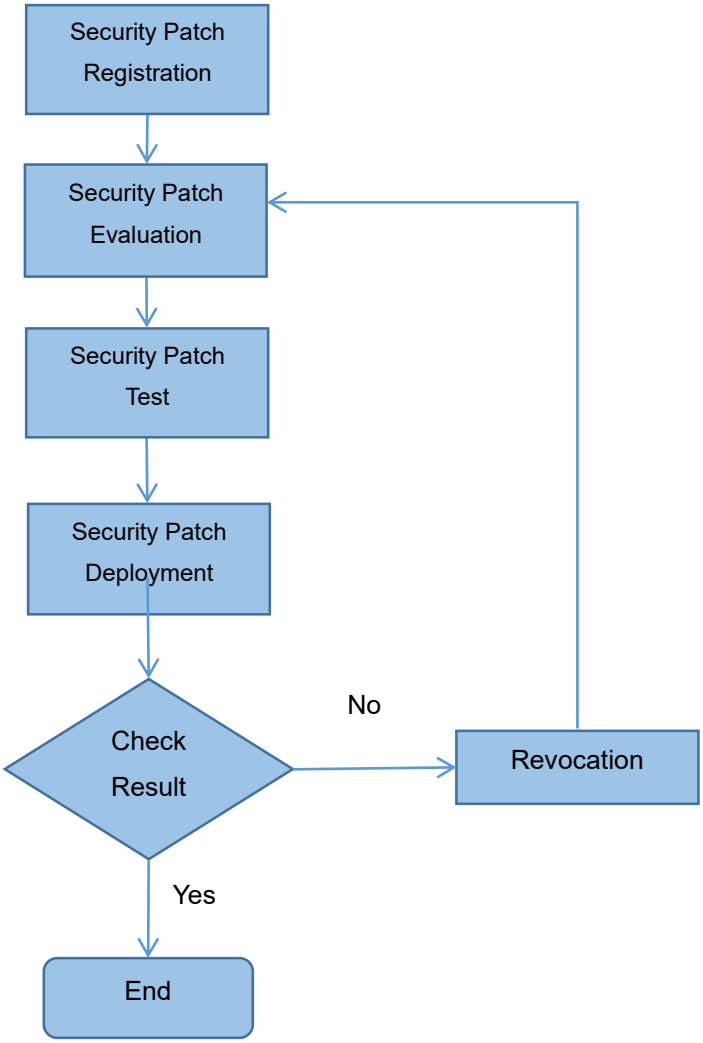
Patch Deployment Timing applies after the registration, evaluation and during the testing steps. The security patch flow can be deployed distributed or centralized to various systems or targets of AccessReal.

2 Flow Details

2.1 Virus Signs

The security patch update flowchart and its descriptions are as shown below.

Note: More introduction about it is located at the later sections of this documents.



No.	Action Name	Action Description	Output	Table
1	Security Patch Collection	Collect patches via official patch release and threaten warnings etc.	Search out the patches needed	Security Patch Record
2	Security Patch Registration	List the system that needs the patch for registration Evaluate the possible patch affected result.	Log the requirement of patch installation	Security Patch Record
3	Security Patch Evaluation	Evaluate the possible patch affected result and risks for the production environment and business. Make a test plan and resources schedule, and notify the system admin.	Patch installation schedule (time/resources)	Security Patch Record
4	Security Patch Test	Test and record the result. Make sure the patch can be implanted to the production environment.	Security Patch Test Report	Security Patch Test Report
5	Security Patch Deployment	Configure patch deployment policy and deploy the patch in the production environment.	Security patch deployment	Security Patch Record
6	Security Patch Revocation	Patch revocation in the production environment if needed.	Evolution Report	

2.2 Security Patch Collection and Registration

The security patch update flow is to manage patch to reduce its effects for business and users while improving the security.

Patches for different systems involves different machines, business flow and so on. So the system admin shall rate the patch level and priority, and report the new patch info to the head of IT department. The IT head will arrange other colleagues to review and evaluate the patch.

Level	Decryption	Action Time
Critical	High attack possibility or the system is being attacked	Deployment shall be done within 12 hours.

Key	Medium attack possibility. The system is not being attacked or its vulnerability is not being used.	Deployment shall be done within 48 hours.
Emergency	There is an attack method, but it's hard to attack.	Deployment shall be done within 1 week.
Serious	There is an attack method, but it's hard to attack. And its damage is limited.	Deployment shall be done within 15 days.
Normal	All other patches except above patches.	Deployment shall be done within 1 month.

2.3 Security Patch Evaluation

Evaluate/review the patch level, risk, effects from the network security, product functions, database security, application system security etc. For the database patch, it's required to add head of IT department, system admin, database admin, AccessReal project head and project manager to form a team to carry out an evaluation.

2.4 Security Patch Test

The patch installation is depending on the evaluation result.

The system admin shall submit the patch test plan if the patch is allowed for deployment. The test plan shall contain test resources, test designs and so on. The test report shall contain test result and the security patch versions.

2.5 Security Patch Deployment

The system admin shall deploy the verified patch, and check the deployment result.

The patches should be downloaded from channels that specified by the company, such as system software/file server or the vendor official website.

The patch deployment execution date is determined by the system admin and IT head. They shall send a notification email to relative staff/department a day before the deployment date. For the critical patch, the email shall be sent 1 hour before the deployment time.

The system admin shall back up all necessary data/file etc. for revocation if deployment fails.

2.6 Security Patch Revocation

The patch revocation is needed if the deployment fails.

The system admin shall check the deployment result and send revocation request to the head of IT department if the deployment fails. The revocation can then be continued only after IT department head approves the request.

The system admin shall inform all related staffs about the revocation of the patch and the possible security issue after a successful revocation.