Australian National University

Procedure: Patch management

Purpose

To establish a procedure for the management of patches to IT services University wide. This procedure applies to all patches including fixes, updates and upgrades.

Definitions

Maintenance window: a period of time designated in advance by Information Technology Services (ITS) or the system owner, during which preventative maintenance that could cause disruption of one or more services may be performed.

Patch: a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities, improve service stability, resolve operational issues; or to provide feature enhancements.

Service: an ICT deliverable, product or component of an overall system. This includes ICT infrastructure, end-user computing devices, operating systems, applications, drivers and firmware.

Procedure

1. This procedure applies to all University owned, leased or ICT managed services.

2. All services are subject to a patch management plan to maintain the reliability and security of ANU resources.

3. All patch management plans adhere to the requirements laid out in this procedure.

4. All patch management plans are approved by the Director, ITS or nominated delegate and integrate into the enterprise's ICT function. In the case of externally hosted services, patch management is incorporated into contracts with the relevant external party.

5. Repeated non-compliance with the approved patch management plan is escalated.

6. The Chief Information Security Officer or Director, ITS may, at their discretion, require any or all system owners to patch the services under their control within a defined timeframe, in response to an imminent threat which indicates this response.

Required components

7. For each service or class of services, the patch management plan contains, or links to:

a. An accurate inventory of every ICT asset and configuration item in the service and identification of which security patches need to be applied whenever suppliers issue them. This includes operating systems, applications, drivers and firmware.

b. Clearly established methods for identifying new patches as they are released by suppliers or internal developers and timetabling their application.

c. Methods for downloading patches from the supplier's primary download source location and verifying the integrity and authenticity of patches.

d. A periodic schedule for patches to be assessed, tested and deployed to the service.

e. A rollback plan, or applicable rollback methods.

f. A deployment plan consistent with the University's change management processes and procedures.

g. Deployment tools which enable the centralised and managed distribution and installation of patches.

h. Options for risk mitigation to be applied to services in an emergency situation where a patch is not available or cannot be applied.

i. Identified alternative mitigation strategies that are implemented as part of the vulnerability management processes. These strategies are subject to a full risk and mitigation planning assessment if required.

j. Additional triggers, periodic reviews, and criteria for initiating major upgrades or product replacement in accordance with the security posture assessment and end of life determination.

Deployment

8. The timeliness of patching reflects the risk and operational requirements of the service. Updates for business critical and internet facing services are considered critical. The timing of all other patches are to consider:

a. operational impact of the service if unavailable;

b. threat risk rating of the service; and

c. the sensitivity of the information stored in the service.

9. Patches are deployed on a schedule that minimises the impact on the function of the service. For example, the following weekly maintenance windows are applied for ITS managed services:

When	Timeframe	Purpose
Tuesday morning	6am – 8am	Updates resulting in potential network disruption.
Tuesday afternoon	2pm – 5pm	For services that are patched during business hours without risk of significant outages.
Tuesday evening	6pm – 3am	Service maintenance for systems and devices.
Thursday afternoon	2pm – 5pm	For services that are patched during business hours without risk of outages.

10. Critical security patches that are urgent and do not fit into established release cycles are applied within 48 hours of a patch release or some alternative mitigation is applied. These changes are considered Emergency Changes by the Change Advisory Board (CAB) and require approval by the Director, ITS. For critical patches on complex services, the patch process commences within 48 hours and takes no longer than two weeks to complete.

11. For the deployment of non-critical patches across large groups of services, or for complex services with multiple environments (such as test, development and production), the patch management plan spreads the patching across available maintenance windows to ensure all levels are updated on a monthly basis. For example:

Week 1	Patching across a sample of low risk services
Week 2	Patching of a larger sample of services once issues are identified and resolved from the previous week

Week 3	The bulk of patching occurs
Week 4	Final round of monthly patching and clean-up from previous groups

12. Following each patch window, successes and failures are assessed with root cause analysis completed for failures when required. In the case of failures, assessment is made to determine whether the patch is applied in the next cycle.

System owner responsibilities

13. System owners:

a. comply with this procedure;
b. are responsible for the establishment and operation of a patch management plan; and
c. are accountable for patching their services.

14. This procedure triggers a requirement for patching, but the decision of whether to patch remains with the system owner except where item 6 of this procedure is applied.

15. Should the system owner choose not to patch, then this decision is made immediately visible to the Director, ITS and Chief Information Security Officer.

Change Advisory Board

16. Prior to implementation, all patch management plans are approved as standard changes by CAB.

17. Deviations from the patch management plan are approved in advance by CAB as a non-standard change. Deviations are considered on a case-by-case basis.

18. Other common administrative tasks related to patch management that require restarts are added as a standard change through CAB and in accordance with the patch management plan.

19. Patching is reported to CAB including progress, successes and failures in accordance with the patch management plan. Automated tools are used where practical, to assist with this reporting. Monthly patching reports are provided to the ITS Executive.

Breaches

20. Identified breaches of this policy and related documents are investigated under the following:

a. Information Infrastructure and Services Rule;
b. ANU Code of Conduct; and/or
c. Discipline Rule.

Document information

Title	Patch Management Procedure
Document Type	Procedure
Document Number	ANUP_5946387
Version	5
Purpose	The policy document is a procedure for the management of patches to IT systems University wide.
Audience	Staff
Category	Administrative
Topic	Information Technology
Subtopic	Security
Effective Date	23 Aug 2019
Review Date	5 Apr 2024
Responsible Officer	Director, Information Technology Services
Approved By	Chief Operating Officer (COO@anu.edu.au)
Contact Area	Information Technology Services (cio@anu.edu.au)
Authority	Information Infrastructure and Services Order 2020 Discipline Rule 2021
Printed On	3 Dec 2023