Technical

London School of Economics & Political Science

IMT

Policy

Patch Management

Jethro Perkins

Information Security Manager

Version	Release 1
Date	09/12/16
Library reference	ISM-PY-141

For latest version and information about, see lse.ac.uk/policies and search by title.

1 Introduction

1.1 Overview

Patching refers to the practise of applying updates to operating systems or applications. Patches typically enhance functionality and close identified security vulnerabilities. It is important, however, to distinguish *patches* from *upgrades*. Patches typically amend the existing code to a release; upgrades may introduce entirely new code. Consequently, LSE's Architecture Board recommends that upgraded software is maintained *at least* at the current -1 upgraded version, while patches (often known formally as security releases) should be kept completely up to date.

1.1.1 Patching and security vulnerabilities

Identified security vulnerabilities are assessed using the "Common Vulnerabilities Scoring System" (https://nvd.nist.gov/cvss.cfm) metric, and consequently assigned a vulnerability rating using the "NVD Vulnerability Severity Ratings"[i] of 'High', 'Medium' or 'Low'.

Identified vulnerabilities are typically kept quiet until a patch is issued, at which point they are made public both through disclosure by the vendor and via lists such as are produced weekly by US-CERT's National Cyber Awareness System.

At the point a vulnerability is considered 'known', both by attackers seeing weaknesses in systems, and by organisations utilising the vulnerable software. Patching therefore becomes a race between attackers looking to exploit unpatched systems and systems administrators seeking to protect them.

Unpatched systems and applications are often a source of compromise, adversely affecting the Confidentiality, Integrity and Availability of LSE data.

Where it is possible, all LSE systems and applications must be updated to the latest patch releases.

1.2 Scope

All LSE systems, servers, workstations, devices and applications.

1.3 Out of Scope

LSE has no mandate to require that personally-owned devices are kept up to date. Unpatched personally-owned devices may, however, be blocked from accessing segments of LSE's network that contain sensitive data.

[i] "1. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9. 2. Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9. 3. Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0."
From 'NVD Common Vulnerability Scoring System' https://nvd.nist.gov/cvss.cfm [accessed 11/10/16]

2 Policy

2.1 Centrally-managed patching

Patching of systems will be centrally-managed wherever possible, unless there are clear business reasons for patching to be performed locally.

2.2 Patches to ‘Critical’ and ‘High’ vulnerabilities

LSE systems, devices and applications must be updated within 30 days of any release of a patch that fixes CVSS-defined ‘High’ vulnerabilities.

Based on the assessed severity and potential / actual impact, the Information Security Manager may mandate a shorter timeframe for any particular instance.

2.3 ‘Medium’ and ‘Low’ vulnerabilities

Patches to CVSS-defined ‘Medium’ and ‘Low’ vulnerabilities must be installed within 30 days of availability, unless mitigating controls are in place to prevent the exploit being realised, in which case the patch may be deferred to the nearest maintenance window.

2.4 Unpatched user devices

Unpatched user devices (laptops, smartphones, tablets etc.) may be blocked from network segments containing sensitive data.

2.5 Exceptions

Some systems cannot be patched, either because they are end of life, rely on a precise software version, or are embedded building management systems (such as ventilation, heating, door management) that are impossible to update.

Exceptions must be recorded and passed to the Information Security Team. Where possible, other hardening techniques will be employed to prevent the compromise of such systems.

2.6 Non-compliant systems

May be quarantined in a network Demilitarised Zone (DMZ) or otherwise switched off.

2.7 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE’s overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE’s website. All staff, students and any third parties authorised to access LSE’s network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

2.8 Review and Development

This policy shall be reviewed and updated regularly by the Information Security Advisory Board (ISAB) and an auditor external to IMT as appropriate to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

For latest version and information about, see lse.ac.uk/policies and search by title.

3 Responsibilities

System Owners
Ensuring patching takes place or otherwise notifying Information Security that patching cannot take place.

Components of a system (e.g. a centrally-managed Operating System, or centrally-managed applications) may have the practise of patching devolved to another team (e.g. IMT systems) but the responsibility of maintaining patching remains with the system owner.

LSE-owned Laptop / Smartphone operators
Ensuring patching of operating system and applications takes place

Department of Information Management and Technology:

- Patching centrally-managed systems and applications.
- Posture checking and network quarantining as appropriate
- Recording unpatched systems
- Removing and / or quarantining noncompliant systems as appropriate

Research Lab
Responsible for the managed patching of RLAB servers, workstations and laptops.

Information Security Advisory Board
Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee
Responsible for approving information security policies.

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy Information Classification Standard	3.12 3.0	06/10/16 15/03/13	Jethro Perkins Jethro Perkins

Version history

Date	Version	Comments
	0.1	Initial version
	0.2	Distributed to Architecture Board members.
	0.3	Incorporating amendments from Head of Infrastructure. Distributed to Nic Warner. Updated STICERD to Research Lab
	0.4	Incorporating amendments from the Applications Architect.
09/12/16	1	Policy approved by Information Technology Committee and moved to release.

Review control

Reviewer	Section	Comments	Actions agreed
Chris Roberts, Head of Infrastructure	2.1, 2.3, 2.4, 3	30 days may be too long for critical patches. Rename “endpoints” to “devices”. Explain BMS/SCADA. Can system owners devolve patching responsibility?	Amend 30 days. Rename endpoints. Explain SCADA. Outline that systems owners can devolve practise but not ultimate responsibility for patching.
Michael D’Urso, Applications Architect	1.0	Distinguish between patches and upgrades. Point out that upgrades should be kept at current -1, whereas patches should always be applied.	Amended as requested.