UNIVERSITY OF PORTSMOUTH

PATCH MANAGEMENT

Jan 2020

Contents

Summary 4
- Who is this for? 4
- How does the University check this is followed? 4
- Who can you contact if you have any queries about this document? 4
- 1.0 Introduction 4
- 2.0 Applicability 5
- 3.0 General Rules 5
- 4.0 Terminology 5
- 5.0 Server (OS) Patching 5
- 6.0 Desktop Patching 6
- 7.0 Application Patching 6
- 8.0 Monitoring
- 9.0 Patch Criticality 6

Document title
Normal text
Document author and department
Normal text
Approving body
Normal text
Date of approval
Normal text
Review date

Normal text		
Edition no.		
Normal text		
ID Code		
Normal text		
Date of effect		
Normal text		
EITHER For public access online (internet)? Tick as appropriate		**YES**
For public access on request copy to be mailed Tick as appropriate	**NO**	**YES**
OR For staff access only (intranet)? Tick as appropriate		**YES**
Password protected Tick as appropriate	**NO**	**YES**
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk		

The latest version of this document is always to be found at:

https://erecords.port.ac.uk/documents

Summary

Information systems require regular updates and on-going technical support. If neglected and allowed to drift out of date, they can become vulnerable to a variety of security threats and/or the system itself can become unstable. Patching keeps IT systems in a state of good 'digital health 'by preventing threats from exploiting vulnerabilities and by removing the vulnerabilities completely.

This advisory explains how patching should be carried out.

Who is this for?

This IS advisory is aimed at service owners and business owners and all those responsible for the operational well-being of IT servers and the services they support.

How does the University check this is followed?

Annual review of this IS advisory will be performed to evaluate its effectiveness.

Who can you contact if you have any queries about this document?

Any questions about this advisory should be directed to servicedesk@port.ac.uk

1. Introduction

'Patching' keeps systems up to date and helps to eliminate many security vulnerabilities and fixes reliability issues. It helps protect the confidentiality, integrity and availability of data. From this point of view, patching is essential to ensure compliance with UK and EU legislation, which demands that owners take reasonable steps to protect data from loss, damage or compromise.

The process of vulnerability detection (scanning) and patching is an on-going but very important process to maintain the digital health of our systems. Unfortunately, as soon as a patch is released, attackers begin to reverse engineer it - in an attempt to identify the original vulnerability and develop exploit code. This process can take a matter of hours or days. ***Over the past few years, most major attacks have targeted known vulnerabilities for which patches already existed but had not been installed.***

2.0 Applicability

This policy covers the rules regarding patching for servers (i.e operating systems), desktop systems and applications. This policy should be read by responsible staff (system owners, local technical support staff and system administrators - including staff in Information Services) who are charged with the maintenance, development and/or support of information systems.

3.0 General Rules

Patching reduces the risk of security breach but there are operational realities to consider - like system downtime and installation overheads. Ideally, patches should be installed immediately after release, but technical issues and resource constraints mean that patching must be prioritised on the basis of risks and impact.

1. Information systems that process personal data must be kept at the highest patch status.
2. Servers and systems subject to DR must be kept at the highest patch status
3. Security systems must be kept at the highest patch status
4. The business owner takes responsibility for the risk management of his/her system, inc. operating system, desktop systems and application software.

If a service is required to be continuously available, the infrastructure that provides that service should be designed in such a way as to allow for patching. This need not require maintenance windows.

4.0 Terminology

Microsoft considers patches as software updates. The standard terminology Microsoft uses for software updates can be found at Appendix B. For simplicity, the general term patch will be used in this document to mean any of the items listed in Appendix B.

5.0 Server (Operating System) Patching

All servers should be subject to routine patching whether being patched automatically via some mechanism (WSUS, ticking the "Patch automatically" checkbox, etc.) or via manual patching regularly.

All exceptions to the standard automatic patching policy must be approved by the IS Security Architect.

In many cases, patching is not complete until the server has been rebooted. So it may be necessary to schedule server reboots.

5.1 Classes of server:

1. Those that are under the direct control of IS:
    1. Servers in pre-production, before handover must be subject to WSUS
    2. Servers provided under the managed service arrangement. In almost all cases, these servers should be subject to automatic update. If special circumstances exist which make WSUS inappropriate, then a risk assessment must be carried out by the Security Architect and the recommendations passed to the risk owner for approval.
    3. Servers that are operated and managed within IS (e.g. DNS, GroupWise, Sophos) These servers must be subject to WSUS.
2. Those that are not directly controlled by IS:
    i. Academic project servers. These servers are wholly owned and managed by members of academic staff and patching is the responsibility of the department.

6.0 Desktop Patching

i. Standard builds

All standard IS built PCs and laptops will be updated with patches that are considered high risk and high impact. All other patches will be incorporated and deployed in new operating system builds. Microsoft Windows patches will be deployed on a monthly basis. Patches will be installed silently, with no need for user intervention.

ii. Non-standard builds

Non-standard PCs and laptops will be updated manually with patches that are considered high risk and high impact.

7.0 Application Patching (Release Management)

Application patching is similar to planned maintenance. Applications are upgraded (rather than patched) as part of a support programme. The steps are:

i. Evaluate upgrade
ii. Plan the implementation
iii. Perform UAT
iv. Release new version

8.0 Monitoring

Responsible staff must take reasonable steps to monitor security mailing lists, review vendor notifications and research specific public web sites for the release of new patches. Advice and support on this can be obtained by contacting the IS Service Desk (ext 7777)

9.0 Patch Criticality

Patch criticality is categorized as follows:

- Emergency — a vulnerability exists and a threat to *the UoP* network is imminent. This is also known as “Patch Now” as the organisation whose assessment of patches we use, will use “Patch Now”.
- Critical — security vulnerability exists but no immediate threat is active.
- Sub-Critical — a routine patch release update.
- Bundle — a collection of fixes which is generally smaller than a service pack

10.0 Deployment

The Desktop Team will choose a suitable method of deployment to ensure that all patches will be deployed to all desktop and laptop PCs. Deployment of patches will be staggered to minimise the risk to corporate systems.
Critical and Sub-Critical patch release requires the creation and approval of a change request before the patch is installed. Relevant SDMs must be informed.
Critical patches can be installed via an emergency change request and the approval of EPS approval. The department will implement Not Critical patches during regularly scheduled preventive maintenance. Each patch will have an approved RTC. As Emergency patches pose an imminent threat to the network, the release is likely to precede testing.

Appendix A – Laptops and users with Administrator Rights

All laptops should be configured to receive patches via the Desktop Teams chosen method of deployment. This will ensure that laptops only receive patches that have undergone our testing. If laptop users choose to install patches that have not been tested and approved by the Desktop Team then the Desktop Team cannot guarantee that any component in the build or any delivered NAL applications will work correctly.

Microsoft Operating System Machines

Patches can be applied using the centrally provided service (WSUS), or through local arrangements, providing there is no appreciable difference in time to update.
ISS will test patches on the second Wednesday each month and release them on the last Wednesday. Those applying patches under local arrangements are to adhere to this schedule.

- Portable computers and those that are only occasionally attached to the network are to be patch maintained.
- Servers with Microsoft operating systems are to be patched within 2 working weeks of patches being released.
- Service packs are to be deployed through the centrally provided system or under local arrangements.
- Service packs are to be tested before release but may be released early when risk justified.

Non-Microsoft Operating Systems

Those responsible for the maintenance or support of non-Microsoft systems must maintain an up to date awareness of vulnerabilities, exploits and patches associated with their platforms.

Routers & Switches

Information Services will keep alert to vulnerabilities affecting the security of routers and switches and securely maintain network equipment for which it has responsibility.

Network Blocking of Non-Updated Computers

Information Services reserves the right to block computers from the network that are not kept full up to date with patches and service packs.

Appendix B - Microsoft terminology for software updates (aka Patches)

Term	Definition
Security patch	A broadly released fix for a specific product, addressing a security vulnerability. A security patch is often described as having a severity, which actually refers to the MSRC severity rating of the vulnerability that the security patch addresses.
Critical update	A broadly released fix for a specific problem, addressing a critical, non-security related bug.
Update	A broadly released fix for a specific problem, addressing a non-critical, non-security related bug.
Hotfix	A single package composed of one or more files used to address a problem in a product. Hotfixes address a specific customer situation, are only available through a support relationship with Microsoft, and may not be distributed outside the customer organization without written legal consent from Microsoft. The terms QFE (Quick Fix Engineering update), patch, and update have been used in the past as synonyms for hotfix.
Update rollup	A collection of security patches, critical updates, updates, and hotfixes, which are released as a cumulative offering or targeted at a single product component, such as Microsoft Internet Information Services (IIS) or Microsoft Internet Explorer. Allows for easier deployment of multiple software updates.
Service pack	A cumulative set of hotfixes, security patches, critical updates, and updates since the release of the product, including many resolved problems that have not been made available through any other software updates. Service packs may also contain a limited number of customer-requested design changes or features. Service packs are broadly distributed and tested by Microsoft more than any other software updates.
Feature pack	A new feature release for a product that adds functionality. Usually rolled into the product at the next release.

Create a patch management group (PMG) to facilitate the identification and distribution of patches within the organization.

The PVG should be specially tasked to implement the patch and vulnerability management program throughout the organization. The PVG is the central point for vulnerability remediation efforts, such as OS and application patching and configuration changes. The duties of a PVG should include the following:

1. Inventory the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization.
2. Monitor security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within the PVG's system inventory.
3. Prioritize the order in which the organization addresses remediating vulnerabilities.
4. Create a database of remediations that need to be applied to the organization.
5. Conduct testing of patches and non-patch remediations on IT devices that use standardized configurations.
6. Oversee vulnerability remediation.
7. Distribute vulnerability and remediation information to local administrators.
8. Perform automated deployment of patches to IT devices using enterprise patch management tools.
9. Configure automatic update of applications whenever possible and appropriate.
10. Verify vulnerability remediation through network and host vulnerability scanning.
11. Train administrators on how to apply vulnerability remediations.

Automated patch management tools.

Widespread manual patching of computers is becoming ineffective as the number of patches that need to be installed grows and as attackers continue to develop exploit code more rapidly. While patching and vulnerability monitoring can often appear an overwhelming task, consistent mitigation of organizational vulnerabilities can be achieved through a tested and integrated patching process that makes efficient use of automated patching technology. Enterprise patch management tools allow the PVG, or a group they work closely with, to automatically push patches out to many computers quickly. All moderate to large organizations should be using enterprise patch management tools for

the majority of their computers. Even small organizations should be migrating to some form of automated patching tool.

Manual methods of patch management.

Manual methods may need to be used for integrating multiplatform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations, operating systems and applications not supported by automated patching tools, as well as some computers with unusual configurations; examples include embedded systems, industrial control systems, medical devices, and experimental systems.

Standardized configurations for IT resources.

Having standardized configurations within the IT enterprise will reduce the effort related to patch management. Enterprise patch management tools will be less effective if deployed within an environment where every IT device is configured uniquely, because the side effects of the various patches on the different configurations will be unknown.

University of Portsmouth
Department of Human Resources
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3141
F: +44 (0)23 9284 3122
E: university.secretary@port.ac.uk
W: www.port.ac.uk