Lancaster University Systems Patching Policy

1. Overview

Lancaster University is responsible for ensuring the confidentiality, integrity, and availability of its data and of any personal data stored on its systems. The University therefore has an obligation to provide appropriate protection against malware threats, such as viruses, ransomware, and worms, which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to University systems.

2. Scope

This policy is primarily aimed at systems administrators and technical support staff who are responsible for the development and maintenance of IT systems and services. However, it also extends to all members of the University who undertake any of the activities covered by this policy.

It is the personal responsibility of individual members of the University to adhere fully with the requirements of this policy. Heads of Departments and Section Heads also have a responsibility to ensure that staff within their department/section comply with the policy.

3. Removal of Insecure Systems

Whenever any system or device connected to the University network presents a perceived risk to University infrastructure, systems or data, Lancaster University reserves the right to remove that system from the network to avoid potential compromise.

Systems that are removed from the network as a result of insufficient patching will be reconnected only when it can be demonstrated that they have been brought up to date and are no longer a risk.

4. Secure Configuration and Patching

All devices that connect to the University's network, regardless of operating system, must be protected from attacks which exploit vulnerabilities within the software through the deployment and installation of software and firmware security patches. Security patches must be installed universally across applicable University systems, within a reasonable timeframe[1] from their available/release, in accordance with this policy. Note that in exceptional circumstances, it may be required to apply critical security patches immediately in order to protect against a serious vulnerability.

[1] Two weeks is considered a reasonable timeframe to apply security patches from release date.

a. Microsoft Platforms

Desktop Patching

All desktop computers connected to the University network must be fully patched and up-to-date. ISS provide central patching for supported versions of Windows. Users and departments must either use this service or patch their machines under their own arrangements. Those who prefer to apply patches under their own arrangements must choose a mechanism that ensures patch delivery in the same time frame as those deployed by the ISS centrally provided patching service. Any user that chooses to apply patches under their own arrangements must be able to demonstrate that they have an effective alternative facility in place.

Patch Testing, Identification and Release

ISS will start testing Microsoft patches following their release on the second Tuesday of every month. If no issues are found during this testing period, ISS will approve the patches for release to all systems using the central patching server[2] within two weeks of initial publication. If problems are discovered with the patches or there are reports from external sources, the impact will be risk assessed and a decision made to determine whether the release should be held back until the issues are resolved.

Deviations to Patch Release

When an exploit to a vulnerability is published prior to the deployment of a patch, a risk assessment will be carried out by ISS, to determine whether it is necessary to apply the patch before it has been fully tested. Where the risk of system compromise is considered to be greater than the impact of deploying of a partially tested patch a decision will be taken to release the patch early.

Where a patched vulnerability presents a significant risk to University systems, an assessment by ISS will be made as to whether the patch installation date should be backdated, forcing the installation to take place.

Patches may be released early or held back during periods when the University is about to close or on a period of change freeze.

Server Patching

Domain joined servers running Microsoft Operating systems should apply security patches within two working weeks of the patches being released. An automated means of patch deployment is the easiest method of achieving this, although time schedules can be chosen by system administrator rather than being fully automated.

---

[2] All ISS Administered and Supported builds use central patching, other domain joined machines will need to check their status.

Users of non-domain joined servers who prefer to schedule patches and restarts under their own arrangements must ensure that their method of patching will fulfil installation in a timely manner so that it is completed in conjunction with the ISS centralised rollout.

b. Non-Microsoft Platforms

Patching Information

Anyone responsible for the maintenance of desktops and servers that run non-Microsoft Operating Systems must ensure that those systems are set to frequently check for updates, and that they are running on a platform that is being supported by the vendor/community.

Classification, Testing and Deployment

Security patches that address vulnerabilities exploitable either remotely or without the use of a user account should be rated as critical and patched in a timely manner. Priority of patching critical vulnerabilities must always be given to systems that are available from off campus.

Patching of Core Infrastructure

ISS staff will subscribe to appropriate security alert e-mailing lists and monitor trusted sources for notification of any vulnerabilities affecting core infrastructure. Where possible patches will be applied only at scheduled maintenance times, in order to avoid any potential impact on people and services using the infrastructure. Where vulnerabilities are found to apply to University core infrastructure, advice may be sought from the University's third party suppliers to determine whether it is feasible to use a work-around solution to enable the patches to be applied according to the normal maintenance schedule. If advice and the outcomes of a risk assessment determine that the patch should be applied immediately, remedial action will be taken. Faculty and departmental computer support staff who operate their own network devices are required to operate their own patch monitoring and deployment in such a way that minimises the risk and potential impact on University systems.

c. Bring your own devices (BYOD) and Internet of things (IOT)

All users are responsible for the maintenance of any personal device connected to the network. Where available, devices should be set up receive updates automatically. Where automatic patching is not available, users should ensure that manual checks occur on a regular basis to ensure the device is both up-to-date and still supported.