جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Vulnerability and Patch Management	Last Review date	19/5/2021
	Policy Number	IT-31	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

A Patch Management Policy comprises of a set of steps and processes aimed towards managing and mitigating vulnerabilities in your environment through a regular and well-documented patching process.

Patch remediation should strictly follow the patch management process for both regular patch updates and critical patch updates.

Scope

This Policy shall be applicable to all platforms being used at the University of Sharjah, including but not limited to Operating Systems, Software applications, Databases and Network devices.

Purpose

The purpose of this policy is to ensure that all University-owned devices are proactively managed and patched with appropriate security updates.

Policy

The patch management process at a minimum should cover Patch identification, Patch testing, Patch deployment and Patch verification.

Patch Identification

IT Operations will use automated tools, where available, to create a detailed list of all currently installed software on workstations, servers and other networked devices. A manual audit and a monthly VAPT will be conducted on any system or device for which an automated tool is not available.

Release of patches by the University of Sharjah vendors shall be monitored effectively by the IT Operations while other relevant critical patches shall be monitored and communicated by the Information Security team.

The University of Sharjah will apply all vendor-provided security patches, which will be installed by the IT operations that manage the systems. All systems will have appropriate software patches to protect against the exploitation and compromise of the University of Sharjah data by malicious individuals and malicious software

IT Operations shall communicate Patch details to the respective Application owners or relevant business owners on a regular basis.

Patching Priority Matrix

The following patch (Microsoft & Operating System) priority matrix represents all systems at UOS, their relative priority for vulnerability patching, and timeframes within which patches must be applied.

System	Criticality	Duration for medium-low patches
Workstations/Laptops	Medium	4 Weeks
DNS/Domain Controller	High	6-8 Weeks
Servers providing web servers	High	6-8 Weeks
Mail Servers	High	6-8 Weeks
Antivirus server	High	6-8 Weeks
Network appliances	High	6-8 Weeks
Other servers & appliances	Medium	6-8 Weeks
Network and Security devices	High	6-8 Weeks

Patch Testing and Approval

System administrators are responsible for testing patches and the Application owners shall be responsible for providing their approvals prior to patch deployment on production. Any application or SAAS services requires patching need to be appropriately agreed between system admin and Application admins.

Where possible, patches will be successfully tested on non-production systems installed with the majority of critical applications/services prior to being loaded on production systems.

Testing must be performed on systems that accurately or near accurately represent the configuration of the production system(s).

Testing of patches shall be completed within 2 weeks from the date of release of the patch.

In case Application owner requires vendor approvals for the patch, they shall send in the written approvals to IT Operations within 2 weeks of the initial communication regarding the Patch from IT Operations.

Only in case of critical patches, IT Operations shall notify the Application owner regarding the patch, however an approval from the Application owner shall not be required prior to critical patch deployment.

Reasons relating to the delay of applying a patch or not applying a patch must be documented and communicated to the Application owner, IT Department Head and Information Security team.

Patch Deployment

1. All patch updates to production environment must follow the University of Sharjah change management process.
2. Change control procedures for the implementation of security patches and software modifications must include the following:
    a. Documentation of impact.
    b. Documented change approval by authorized parties.
    c. Functionality testing to verify that the change does not adversely impact the security of the system.
    d. Rollout plan
    e. Back-out procedures
3. The administrator shall perform a full backup of critical systems to be patched before applying the patch.
4. System state backup /snapshots shall be taken before deploying patches.
5. Roll back plan should be ready if patch/update/hot-fix fails on production/testing environment.
6. System and device patches must be automatically deployed through the use of Enterprise Patch Management solution.
7. Systems and devices that are not supported by the Enterprise Patch Management solutions (Network devices etc.) or with non-standard configurations must be patched manually by the system administrators
8. All identified critical patches shall be applied within 24 hours for systems that are facing internet including servers in the DMZ, Firewall, IDS/IPS, E-mail Server, Web Gateway, extranets
9. All identified critical patches shall be applied within 24 hours for internal systems including desktops/laptops.
10. All other patches shall be applied within 30 days for systems that are facing internet including servers in the DMZ, Firewall, IDS/IPS, E-mail Server, Web Gateway, extranets
11. All other patches shall be applied within 30 days for internal systems including desktops.
12. Patches will be applied during an authorized maintenance window as agreed with the Application owners

Patch Verification

1. Systems and devices shall be reviewed by the administrator to verify successful application of patches and in compliance to vendor documentation for the specific patch.
2. Application owners would need to inform IT Operations within a day of the production patch deployment, if the application is working successfully or not.
3. Logs will be maintained for all system categories (servers, desktops, switches, etc.) indicating which devices have been patched. System logs help record the status of systems and provide continuity among administrators. Information to be recorded will include but is not limited to: date of action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator's remarks.
4. All configuration and inventory documentation must be immediately updated in order to reflect applied patches.
5. Audits should be performed to ensure that patches have been applied as required and are functioning as expected.
6. A patch addressing following vulnerabilities shall be considered critical

Type of Vulnerability	Priority
Remote Exploitable Vulnerabilities	Critical
Providing Remote Access to Systems	Critical
Provides Privileged Access to Systems	Critical
Authentication is not required to exploit the vulnerability	Critical
Total Information disclosure resulting in all systems files being revealed	Critical
Complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.	Critical
Total shutdown of the affected resource. The attacker can render the resource completely unavailable.	Critical
Patches categorized as critical by vendors.	Critical

Reference

Standard	**Control Ref**
ISO 27001:2013	A.12.6.1,