Southwestern Oregon Community College

AP11010 Patch Management

This procedure provides clarification about patching strategy, and whether all patches should be automated, manual, or default. There has to be a classification based on the seriousness of the security issue followed by the remedy. Patch Management is a set of generalized rules and solutions. The idea is to have a process in place to prevent and resolve existing issues. .

The procedure applies to all components managed by IT Department infrastructure and includes Computers, Servers, Software, and Switches, Peripherals, Databases and Storage. Users should be made aware of the procedure. Administrative and IT staff are responsible to keep the system clean and safe and ensure the patches are updated regularly.

Periodical reviews on the supplier's website who provides servers, PC's, tablets, printers, switches, routers and other peripherals, check firmware patches. The IT Department will be responsible for the approval of all the patches and take ownership of all technical updates starting from operating systems, software, antivirus, servers, workstations, patches, and drivers of devices.

Implementing this procedure effectively reduces the likelihood of compromise. The end user has a responsibility to ensure that patches are installed, and the machine is rebooted in a timely manner. The end user also has the responsibility to report problems to ITS. Once the ITS systems are in production, third party suppliers must ensure vulnerability patching is carried out.

Microsoft security updates are released on the second Tuesday of each month. Patches will be released as soon as possible.

The first step in Patch Management is to define your starting point and to identify and categorize your assets: taking a full inventory of all workstations and servers on your network.

Inventory report should involve the list of assets with OS version and application installed on it. Once your assets are identified, they need to be categorized based on exposure and risk. By categorizing assets, you develop a picture of which machines require rapid patch management (within hours or days) and which require standard management (weeks.) Categorizing your assets is almost always a manual process. It is difficult to automate a process that essentially identifies “important machines” and “less-important machines.”

The CIO is authorized to limit network access for individuals or units not in compliance with all information security policies and related procedures. In cases where College resources are actively threatened, the CIO should act in the best interest of the College by securing the resources in a manner consistent with the Information Security Incident Response Plan. In an urgent situation requiring immediate action, the CIO is authorized to disconnect affected individuals or units from the network. In cases of noncompliance with this procedure, the College may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

This IT procedure, and all policies referenced herein, shall apply to all members of the College community including faculty, students, administrative officials, staff, alumni, authorized guests, delegates, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, the College's IT Resources, whether individually controlled, shared, stand-alone, or networked.

Any systems within the IT scope must be part of a patch management cycle.

The term IT systems includes:

- Workstations
- Servers (physical and virtual)
- Firmware
- Networks (including hardwired, Wi-Fi, switches, routers etc.)
- Hardware
- Software (databases, platforms, etc.)
- Applications
- Cloud Services

When a vulnerability is identified, patches will be deployed as soon as possible.

Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to the following:

- Updating software
- Fixing a software bug
- Installing new drivers
- Addressing new security vulnerabilities
- Addressing software stability issues

Exceptions to the patch management procedure require formal documented approval from the Change Management Team. Any servers or workstations that do not comply with procedures must have an approved exception on file with ITS. Requests for exceptions should be made to the ITS Director for Infrastructure and Enterprise Application Services.

1. **Purpose**
   Southwestern is committed to providing a secure computing environment and understands that vulnerabilities need to be remediated and managed. It only takes one device to threaten the security of all computers and other devices on the network. Patching and vulnerability scanning is necessary to help prevent exploitation with the organization. Being proactive will help reduce or eliminate potential exploitation and may reduce the time it takes to remediate an exploitation if it occurs. Patching usually requires a reboot to complete the installation. Users should always be saving their documents periodically as a best practice.
2. **Servers, Firewalls, Load Balancers, Wi-Fi/Access Points, Web Application server, Storages, Databases**
   All updates will be installed when possible. Patches labeled critical/high will be installed within 30 calendar days or as soon as possible. Patches labeled as high/medium or non-critical will be installed within 90 calendar days. Low priority should be installed within 90 calendar days or longer depending on the system. Whenever possible, patches should be tested on development or non-production environments before applying to the production environment. Patches taking longer than 90 days must be approved by the CIO or assignee. Every quarter deferred patches will be reviewed.
3. **Vendors**
   All vendor-maintained systems/applications that are of critical or high nature must be patched within 90 days of the approved release from the vendor. Any non-critical patches may be installed on a case-by-case basis.
4. **Vulnerability Scans**
   After patching or remediating vulnerabilities, a scan will be performed to show that the patches were installed correctly.
5. **Endpoints**
   All Southwestern owned endpoints are to have critical operating system and application patches installed within 30 calendar days of release from the vendor.
6. **Scheduling and Deployment**
   Patches will be tested prior to deployment on campus. Communication to campus regarding security patches will be emailed monthly to the College approved list serve such as General Announce.
7. **Emergency Updating**
   Periodically a highly critical software update will be released outside of normal patch times. If this exploit may affect a large number of users, the patch may be pushed out within one day of release. Communication to campus regarding security patches will be emailed as necessary to the College approved list serve such as General Announce.

Adopted: April 21, 2021