**University of Alabama at Birmingham**

**PATCH MANAGEMENT RULE**

Approved and Implemented: June 20, 2019

Reviewed/Updated: February 12, 2021

**Related Policies, Procedures, and Resources**

[Data Protection and Security Policy](https://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000038.aspx)

[Data Access Policy](http://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000789.aspx)

[Acceptable Use Policy](http://www.uab.edu/policies/content/Pages/UAB-IT-POL-0000004.aspx)

[Data Protection Rule](http://www.uab.edu/it/home/component/k2/item/818-data-protection-rule)

[Minimum Security for Computing Devices Rule](https://www.uab.edu/it/home/images/UAB_Computing_Device_Standard_2017_Final.pdf)

[Vulnerability Management Rule](https://web.ad.uab.edu/policies/content/Pages/Vulnerability-Management-Rule.aspx)

**1.0 Introduction**

Patch management is a critical preventive measure designed to proactively counter the exploitation of vulnerabilities that exist within UAB systems. By taking a proactive approach to managing vulnerabilities, the University is able to reduce or eliminate the potential for exploitation and prevent the excessive time, effort, and costs that result when responding to an incident after it has occurred.

Patching may require systems to be rebooted in order for the patch to be applied. Commensurate with this, the disruption to the systems being patched should be minimized by using a preferred window of weekends.

**2.0 Scope and Applicability**

All UAB-owned devices as well as devices that store, process, or transmit University data must be proactively managed and patched with appropriate security updates.

**3.0 Patch Management**

1. Endpoints
   * + - 1. Patch management for all endpoints is centrally managed by UAB IT.
         2. All critical operating system and application patches will be installed within thirty (30) days of release from the vendor.
         3. UAB IT will prioritize centralized patching efforts in the order of (1) Windows operating systems, (2) Apple operating systems, (3) applications such as Adobe, Flash, etc.
         4. Application software vendors release security patches on a regular schedule. For centrally managed devices, applicable patches will be tested and validated by UAB IT prior to deployment to campus. Once validated UAB IT will schedule and deploy validated patches to end points on a monthly basis. UAB IT will communicate with the campus community regarding deployed security patches.
2. Servers
   * + - 1. All university-managed servers will be maintained with the latest security patches to their operating systems and applications.
         2. Each service owner is responsible for UAB servers under their control. Each UAB server must have a named service owner and system owner. When a patch is announced, an authorized system owner must document the change according to formal change management procedures. The service owner must assign a criticality rating based on their experience, the classification of the data (per UAB Data Classification Rule) contained on the server, and the level of risk to the institution in the event of compromise.
         3. All high/critical patches must be applied as soon as practically possible. This period shall not exceed thirty (30) calendar days after public release for any business critical production server.
         4. All medium criticality patches or patches for non-critical systems must be applied within sixty (60) calendar days.
         5. Any low criticality patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible.
         6. In cases where patching cannot follow the standard as outlined above, an exception request form must be completed and submitted to the UAB Chief Information Security Officer (CISO) for approval. These exception requests will only be approved for a maximum of three months and will follow the normal exception request process.
         7. All patches for vendor-maintained systems/applications that are labeled as high/critical must also be patched within thirty (30) days of the approved release from the vendor. The UAB operating unit is responsible for maintaining knowledge of these patches and ensuring that vendors comply with this standard.
3. Endpoint Procedures
   * + - 1. Installation and Validation
   1. A system reboot is required to successfully install most security patches. Until the reboot occurs, the computer will remain vulnerable to attacks which the installed patch protects against. Security updates will be deployed using regularly occurring weekend maintenance windows. UAB IT recognizes that flexibility may be needed around a system reboot to provide the university community with the option to reboot with minimal impact to productivity and operations. Because of this, exemptions will be allowed if requested, provided there is a valid business case.
   2. There are two exemption methods that will allow users to install scheduled updates at their convenience within a pre-determined time-frame.
      1. Users will be provided five (5) business days to select the installation time of their choice for patching. Should the five (5) business days pass without the necessary reboot, updates will automatically install and may enforce reboots of the computer, as the updates require. In order to ensure that end points are protected, and work is not disrupted due to reboot, it is strongly recommended that users install the updates as soon as possible. When updates are available, they will appear in the system tray. This is the preferred update method if an exemption is required.
      2. In the event that the five (5) business exemption window for patch application could have a negative impact on academic or operating unit processes a special exemption may be granted. Users that feel this is the case may request to be temporarily exempted from the mandatory reboot process. If an exemption is granted, endpoints will still have patches deployed regularly, but it will be the end user's responsibility to install updates and reboot the machine. Updates will be presented in the same way as the first exemption option; however, the automatic install and reboot is extended to 30 days.
   3. Out-of-Band Updates
      1. On occasion, a software vendor will release a critical security patch outside of their normal release cycle. The usual reason for the release of an out of band patch is the appearance of an unexpected, widespread, destructive exploit that will likely affect a large number of users. In the event of a published out-of-band patch, UAB IT will expedite the validation process. Once validated, users will have one (1) business day to install and reboot their machine to apply the patch. In the event that the deadline passes, updates will automatically install and may enforce reboots of your computer as the updates require. UAB IT will communicate with the campus community in the event of an out of band update deployment.
4. Server Procedures
   1. Installation and Validation
      1. A system reboot is required to successfully install most security patches. Until the reboot occurs, the server will remain vulnerable to attacks which the installed patch protects against. Security updates will be deployed using regularly scheduled weekend maintenance windows within a quarter of release, and for business critical services should be validated in a development environment first.
   2. Out-of-Band Updates
      1. On occasion, a software vendor will release a critical security patch outside of their normal release cycle. The usual reason for the release of an out of band security patch is the appearance of an unexpected, widespread, destructive exploit that will likely affect a large number of users. In the event of a published out-of-band security patch, the validation process should be expedited as well as the installation and reboot of the server.

4**.0 Enforcement**

Each University academic and business unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard security rule.

The Vice President of Information Technology Office is responsible for enforcing this standard security rule.

Any device which is not updated as outlined in this standard may be removed from the UAB network, disabled, etc., as appropriate until the device can comply with this standard or an exception request be approved.

**5.0 Exceptions**

Exceptions may be granted in cases where security risks have mitigating controls in place to lessen the intensity from a critical to a minimal level. To request a security exception, complete the UAB Security Policy Exception request from the UAB IT Tech Help portal.

**Change History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Description** | **Approval** | **Date** |
| 1.0 | Initial document | Dr. Curt Carver | 6/20/2019 |
| 2.0 | Paragraph 3.11.b – changed automatic install and reboot to 30 days for granted exceptions to normal patch schedule | Dr. Curt Carver | 6/24/2020 |
|  | Reviewed - no changes/updates |  | 2/12/2021 |
|  |  |  |  |
|  |  |  |  |