Patch Management Standard

1. **Overview and Purpose**

This document describes the minimum requirements for maintaining up-to-date operating system and vendor software patches on all Esri owned and managed devices including servers, firewalls, network switches and routers, database and storage systems. The purpose of this document is to provide standards and frequency for application of critical security updates and patches and reacting to any discovered vulnerabilities.

1. **Scope**

This policy applies to all non-classified assets owned or managed by Esri.

1. **Patch Management**

Roles and responsibilities for personnel executing the Patch Management Standard is broken down below according to the table

|  |  |  |
| --- | --- | --- |
| **Entity** | **Patch management Role** | **Operational Responsibilities** |
| System Owners | System owners are responsible to ensure their systems are patched and complies with the Patch Management Standard. They work with infrastructure and operations and security operations to create exception when required and implementing acceptable mitigating controls to reduce risks for systems under exceptions. System owners are also required to ensure accurate inventory of the systems they managed in ServiceNow. | * Manage systems inventory in ServiceNow * Review patches from the vendors to ensure the systems are up to date on patches. * Assess operational impact on implementing the patches. * Reviewing and mitigating risks to the system which are in exception from patching standard. |
| Security Assurance | Security Assurance works with system owners in the event a system cannot comply with the standard. The team will review any exception that are requested by system owners and ensure appropriate mitigating controls are in place. | * Review exception requests and manage associated risk. |

Minimum patching frequency for each type of system is listed in the table below. In the event security patches are required, the timing of patching will be determined as described in section 4.

|  |  |  |
| --- | --- | --- |
| **System Type** | **Patch management schedule** | **Patch Type** |
| Windows Server | Monthly | Operating system Patch and Security updates |
| Linux and Unix based Servers | Monthly | Operating system Patch and Security updates |
| Databases | Monthly | Security updates |
| All other systems including but not limited to firewall, network switches and routers, storage systems and others | Monthly | Firmware and security updates |

**3.1 Exception to Patching Standard**

In circumstances where compliance with some or all of the Patching Standard is not achievable in the immediate term, an exception must be documented and approved. This will require completion of an [Exception Request](https://esri.service-now.com/sp?id=sc_cat_item&sys_id=877ce579dbe09c508a123a4b7c9619fb&sysparm_category=5040eb10db5a6300ad7f92c6db96196d) form.

Each system owner will document their patching schedule and submit exception requests for any deviations from the standard schedule. Exceptions must be requested in case a system is not being updated to the latest available patch even though the above patching schedule is followed.

Unsupported application or operating systems are still subject to patching requirements. If vendor support or community support ceases then an exception request must be made.

**3.2 Monitoring and Tracking**

Systems must be monitored to ensure that the patches have been applied. ServiceNow will employ an automated method for reporting the patching compliance. The system owner will ensure all their systems are discovered in ServiceNow. The system owner is responsible for ensuring patch levels are following the standard.

**3.3 Patch Lifecycle Management**

While critical vulnerabilities or bugs will need immediate remediation, we need to keep up to date with new software releases and patches for all our systems.

Most major vendors put out Security Advisories when a vulnerability is discovered and/or a new patch is released. System owners will have to track and review new software releases and security advisories every 30 days. System owners must sign up for an e-mail notification from vendor when available and optionally have a regular cadence call with the vendor.

System owners will document the process they use to keep up to date with new software releases, security advisories and patches for all our systems.

**3.4 Confirmation of Closure**

## ServiceNow will generate tickets for any system that falls out of compliance with the Patching Standard. A standard SLA of 14 days will be applied to these tickets and the system owner would act upon these tickets by either applying the required patch or requesting exception.

1. **Vulnerability Management**

Roles and responsibilities for personnel executing the policy will be broken down according to the table below:

|  |  |  |
| --- | --- | --- |
| **Entity** | **Vulnerability Management Role** | **Operational Responsibilities** |
| **Vulnerability Management Team** | The Vulnerability Management ensures that in-scope systems are scanned for vulnerabilities on a regularly scheduled basis and that identified vulnerabilities are prioritized according to the risk posed to the organization and reported to the personnel responsible for patching the affected system(s). | * Manage Tenable.io * Analyze & prioritize vulnerability scan data and disseminate reporting. * Issue prioritized remediation recommendations and guidance to Infrastructure & Operations Team. * Track the vulnerability resolution progress. * Report unmitigated vulnerabilities of significance to leadership. |
| **Risk Owners** | Risk Owners own the risk associated with a specific set of systems or applications. They work with Infrastructure & Operations to authorize, prioritize, and schedule changes to their systems, or implement acceptable mitigating controls to reduce the risk per the guidance of the Vulnerability Management team. | * Review vulnerability reports. * Review corrective actions or mitigating controls recommended by Vulnerability Management team. * Assess the operational impact of the proposed remediations. * Schedule remediations and configuration changes with responsible patch teams and end users. |
| **Infrastructure & Operations Team** | Infrastructure & Operations patch teams implement corrective actions recommended by the Vulnerability Management Team and authorized by the Risk Owners. They are technical resources that may research and  propose various resolutions and mitigating controls. | * Review vulnerability reports. * Propose corrective actions or mitigating controls to the Risk Owner(s). * Implement changes recommended by Vulnerability Management team and authorized by the Risk Owner(s). * Implement recommended changes in the timeframe dictated by the Patch Management Policy. * Provide technical justification for vulnerability exceptions as needed. |

When available, Tenable’s Vulnerability Priority Rating (VPR) score will be used as the primarymetric for prioritizing patches.

Additionally, patches will be deployed using a risk-based approach, specifically taking into

account the following:

* Criticality of the affected asset(s) to business operations and/or sensitivity of resident data.
* Threat intelligence provided by Tenable via Vulnerability Priority Rating (VPR) which is a dynamic value that augments a vulnerability’s CVSS score by factoring in threat metrics such as exploitability, likelihood of attack, etc.

The Risk Triage Matrix below will serve as the primary mechanism for prioritizing vulnerabilities and prescribing an appropriate response from the responsible patch team:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Category** | **Definition** | **Criteria** | **Response** | **SLA** |
| **Emergency** | Exposure poses imminent and unacceptable risk to:  • Tier 1 systems  • Critical Business Service(s)  • Public-facing systems (Perimeter/DMZ) | • VPR 9-10  • Exploit (any of the following)  -Available  -Forthcoming  - Existing tools (Exploit Kit)  • No mitigations or workarounds available | Emergency patching of all affected  systems (Tiers 1-3) | ≤7 Days |
| **Critical** | Exposure poses urgent & unacceptable risk to:  • Tier 1 systems  • Critical Business Service(s)  • Public-facing systems (Perimeter/DMZ) | • VPR 7-8.9  • Exploit (any of the following)  - Available  - Forthcoming  - Existing tools {Exploit Kit)  • Mitigations available | • Emergency patching of affected Tier 1  systems  • Normal patch schedule for all other affected systems | * ≤7 Days (Tier 1) * ≤30 Days |
| **High** | Exposure poses likely and partially acceptable  risk pending successful remediation or  mitigation | • VPR 4-6.9  • Exploit difficult to execute or non-existent  • Mitigations unavailable or difficult to implement  (Operationally unfeasible) | • Patching required  • Normal patch schedule for all affected systems  • Long-term mitigation unacceptable | ≤60 Days |
| **Moderate** | Exposure poses an acceptable amount of risk  pending successful remediation and mitigation | • VPR<4  • No known exploit  • Theoretical vulnerability  • Mitigations easily implemented | • Patching optional  • Normal patch schedule for all affected systems  • Long-term mitigation plans acceptable | ≤90 Days |

* 1. **Vulnerability Management**

|  |  |  |
| --- | --- | --- |
| **Risk Category** | **Confirmation Process** | **SLA** |
| **Emergency\Critical (Tier 1)** | Upon completion of remediation a task should be created in ServiceNow requesting VM team to rescan objects and report findings | ≤24hrs |
| **Critical** | Operations to validate remediation is complete. VM team will monitor via regularly scheduled scanning and report additional findings as needed. | ≤30 Days |
| **High** | Operations to validate remediation is complete. VM team will monitor via regularly scheduled scanning and report additional findings as needed. | ≤60 Days |
| **Moderate** | Operations to validate remediation is complete. VM team will monitor via regularly scheduled scanning and report additional findings as needed. | ≤90 Days |

## Exceptions Management

Vulnerabilities may exist in operating systems, applications, web applications, or in the way

different components interoperate. While every effort must be made to correct issues, some

vulnerabilities cannot be remediated.

In these cases, additional protections may be required to mitigate the vulnerability. Exceptions

may also be made so that the vulnerabilities are not identified as items of risk to the system

and organization. These types of shortcomings don’t accurately reflect the risk of a system and

require an exception process. This elaborates itself in the form of two primary exception types:

|  |  |  |
| --- | --- | --- |
| **Exception Category** | **Description** | **Response** |
| **Accepted Risk** | Legitimate vulnerabilities left unpatched because compensating controls are in place to mitigate the risk, a hosted service has been deemed too critical for intervention, an asset has been scheduled for decommissioning, etc. | Risk acceptance exceptions must be requested through the  Security Assurance team with an explanation containing:   * Mitigating controls - what changes, tools, or procedures have been implemented to minimize the risk. * Risk acceptance explanation - details as to why this risk is not relevant to the company and affected systems/applications. * Risk analysis - if the vulnerability is indeed compromised, what data and/or systems/applications will be affected. |
| **Delayed Action** | Legitimate vulnerabilities that cannot be mitigated in the time frame specified by the SLA due to business impact (downtime to apply remediation) or because testing is required to ensure operations are not affected by the recommended remediation. | Delayed Action exceptions require a plan to test the  recommended remediation and a date that corrections can be  implemented without negatively impacting business operations. |

All exception requests must be submitted via ServiceNow for review and adjudication. All

exception requests must present a technical or operational justification and an expiration date.

No exception can be permanent, and each must be reviewed and extended using an expiration

date to ensure no exceptions are permanently ignored. The request should clearly state the

exception type and be recorded in both ServiceNow and Tenable.io

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version Revised | Revised by | Reason for Revision |
| 1/17/2023 | 2.1 | Nicholas Luebbers | Clarify EOL exception equirements |
| 5/1/2022 | 2.0 | Shreyas Ramesh | Incorporate Patch management into current vulnerability management contents |
| 3/9/2021 | 1.1 | Nicholas Luebbers | Periodic review |
| 11/10/2017 | 1.0 | Matt McClung | Initial Version |