Vulnerability Management

Standards Document

Version 1

Produced:
March 10th, 2023

Edited:
April 19th, 2023

Written by:
Miguel Suárez - Security Officer

Approved by:
Paula Amador - Chief Product Officer

1. Policy Statement

Expresia is committed to maintaining a secure and reliable environment by effectively mitigating potential vulnerabilities that may impact our systems and operations. To achieve this, we have developed and implemented a robust Vulnerability Management Standard, which aims to ensure that all vulnerabilities are promptly identified, accurately assessed, and remediated in a timely and efficient manner.

2. Risk Assessment

We conduct regular risk assessments to identify potential vulnerabilities that may impact our systems and operations. This includes identifying potential threats, assessing the likelihood of exploitation, and the potential impact on our systems and operations. The results of the risk assessments will be used to prioritize vulnerability remediation efforts.

3. Vulnerability Scanning

We conduct regular vulnerability scans on all systems and applications to identify potential vulnerabilities. The scans will be conducted using industry-standard tools and will be scheduled to minimize disruption to our operations.

All vulnerability scan results will be recorded in a vulnerability tracking tool, such as an Excel spreadsheet or Jira issue tracker. The header should include the date of the scan, the system/application scanned, the scanner used, and the vulnerabilities identified. If a CVE exists, it is appended to the vulnerability's description.

We pay special attention to the OWASP web application vulnerability list in the web application, as well as important business flows in the application. Manual testing is preferred over automated testing using BurpSuite, widely recognized as one of the premier tools in the web application security industry. Automated testing is done as an addition to it, using open source pentesting tools such as sqlmap.

4. Vulnerability Remediation

The goal of the Vulnerability Remediation process is to ensure that all vulnerabilities identified during scanning are addressed in a timely and effective manner to reduce the risk of a security incident. The following procedures will be followed for prioritizing and remediating vulnerabilities:

1. **Prioritization of vulnerabilities:** All vulnerabilities will be classified based on their severity level, as determined by the vulnerability scanner, and their potential impact on the organization's systems and data. The severity level and impact assessment will be based on a predetermined scale, which will be documented in the organization's Vulnerability Management Standard. The scale should be aligned with industry-standard frameworks and best practices. Prioritization may vary also depending on the context of the vulnerability.

2. **Remediation plan:** Based on the severity and impact assessment, a remediation plan will be developed for each vulnerability. The plan will include a timeline for remediation, the resources required to remediate the vulnerability, and the individuals responsible for remediation.
3. **Remediation execution:** The team responsible for remediating the vulnerability will execute the remediation plan according to the established timeline. This may involve installing patches, updating configurations, or implementing other measures to mitigate the vulnerability. All remediation activities will be documented, and the status of each vulnerability will be updated in the organization's vulnerability tracking system.
4. **Verification and validation:** Once the remediation activities have been completed, the team responsible for remediating the vulnerability will verify and validate that the vulnerability has been successfully mitigated. This may involve re-scanning the system or conducting other tests to confirm that the vulnerability is no longer present.

Thus vulnerabilities are prioritized based on their severity and potential impact, and are promptly remediated to reduce the risk of a security incident.

5. Patch Management

The Patch Management process is critical for maintaining a secure environment by addressing vulnerabilities in software applications and operating systems. The following procedures will be followed for managing and applying software patches and updates:

1. Identification of patches: The IT team will identify and review available patches and updates on a schedule, using sources such as vendor websites, security advisories, and industry publications. Patches will be classified based on their severity level, and their potential impact on the organization's systems and data. The severity level and impact assessment will be based on the affected service role and context, which will be documented and tracked accordingly.
2. Patch management plan: Based on the severity and impact assessment, a patch management plan will be developed for each patch. The plan will include a timeline for patching, the resources required to patch the vulnerability, and the individuals responsible for patching.
3. Patch deployment: The IT team will deploy the patches according to the established timeline. This may involve testing the patch on a non-production system to ensure that it does not cause any issues before deploying it on production systems. All patching activities will be documented, and the status of each patch will be updated in the organization's patch tracking system.
4. Verification and validation: Once the patch has been deployed, the IT team will verify and validate that the patch has been successfully installed and that the vulnerability has been addressed. This may involve re-scanning the system or conducting other tests to confirm that the vulnerability is no longer present.
5. Rollback plan: In the event that a patch causes unexpected issues, the IT team will have a rollback plan in place to revert the system to its previous state. This will minimize the impact on the organization's systems and data.

By following these procedures, Expresia ensures software patches are promptly identified, assessed, and deployed to address vulnerabilities, reducing the risk of a security incident.

6. Configuration Management

The Configuration Management process is essential for maintaining a secure environment by managing the configuration of systems and applications to reduce the risk of vulnerabilities being introduced. The following procedures will be followed for managing the configuration of systems and applications:

1. Configuration baseline: The IT team will establish a configuration baseline for all systems and applications, including hardware, software, network devices, and security settings. The baseline will be regularly reviewed and updated as necessary to reflect changes in the IT environment.
2. Configuration change management: All configuration changes will be managed through a formal change management process. Requests for changes to the configuration baseline will be submitted to the IT team, reviewed for their potential impact, and approved or denied based on their alignment with the organization's security policies and standards.
3. Configuration monitoring: The IT team will monitor the configuration of systems and applications to ensure that they remain in compliance with the configuration baseline. Configuration monitoring will include automated tools and manual checks to identify any unauthorized changes or deviations from the baseline.
4. Configuration hardening: All systems and applications will be hardened according to industry-standard guidelines and the organization's security policies. Hardening will include measures such as disabling unnecessary services and protocols, removing default accounts and passwords, and enabling security controls such as firewalls and intrusion detection/prevention systems.
5. Configuration backup and recovery: The IT team will establish a backup and recovery strategy for all systems and applications to ensure that configuration data can be restored in the event of a system failure or security incident.

Configuration of systems and applications is managed in a way that reduces the risk of vulnerabilities being introduced. Regularly reviewing and updating the configuration baseline, managing changes through a formal process, monitoring for unauthorized changes, and hardening systems and applications according to industry standards and security policies can help prevent security incidents and protect the organization's systems and data.

7. Incident Response

The Incident Response process outlines the procedures for responding to security incidents involving vulnerabilities. These procedures include escalation procedures, communication plans, and incident response testing. The following steps will be taken in response to security incidents:

1. **Incident identification and reporting:** All employees are responsible for identifying and reporting security incidents to the Expresia team as soon as possible. Incident reports should include a description of the incident, the affected systems and data, and any relevant information about the cause or impact of the incident.
2. **Incident response team:** The Expresia team will establish an incident response team (IRT) consisting of trained personnel who will be responsible for responding to security incidents. The IRT will include members from various departments, including IT, legal, and management.
3. **Incident assessment and triage:** The IRT will assess each reported incident and prioritize its response based on its severity, potential impact, and the systems and data affected.
4. **Incident containment and eradication:** The IRT will take immediate steps to contain the incident and prevent further damage to the organization's systems and data. The IRT will also work to eradicate the vulnerability that was exploited in the incident.
5. **Incident recovery and follow-up:** The IRT will work to restore the affected systems and data to a secure state. After the incident has been resolved, the IRT will conduct a follow-up review to identify any lessons learned and to make recommendations for improving the incident response process.
6. **Incident escalation and communication:** The IRT will establish procedures for escalating incidents to senior management and external stakeholders, such as customers and regulatory agencies. The IRT will also establish communication plans for keeping stakeholders informed about the incident and its resolution.
7. **Incident response testing:** The incident response plan will be regularly reviewed, updated, and tested to ensure that it remains effective and that the IRT is prepared to respond to security incidents.

This way, security incidents involving vulnerabilities are responded to promptly, efficiently, and effectively. The incident response process includes incident identification and reporting, IRT formation and training, incident assessment and triage, incident containment and eradication, incident recovery and follow-up, incident escalation and communication, and incident response testing.

Specific details regarding timing and forms of communication are described in all client service level agreements.

8. Roles and Responsibilities

To ensure that all vulnerabilities are managed effectively, it is important to clearly define the roles and responsibilities of employees and other stakeholders in managing vulnerabilities. The following roles and responsibilities have been established:

- Chief Technology Officer (CTO): Responsible for overseeing the development, implementation, and maintenance of the Vulnerability Management Standard. The CISO should ensure that the standard aligns with organizational objectives and is in compliance with regulatory requirements.
- Expresia Technical Lead: Responsible for coordinating with the Vulnerability Management team, and makes sure that the standard is integrated into operational processes.
- Director of Infrastructure: Responsible for ensuring that IT systems and infrastructure are configured securely to reduce the risk of vulnerabilities being introduced. Making sure access controls, firewalls, and secure protocols are in place throughout the infrastructure.
- Security Officer: Responsible for ensuring that appropriate security measures are in place to protect Expresia and customer data from vulnerabilities. This includes auditing processes to avoid unauthorized access to Expresia systems and data. Ensures that the standard is up-to-date and effective and works with the IT team to mitigate technical risks. Manages the day-to-day operations related to vulnerability management.
- IT Support Specialist: Responsible for identifying and reporting vulnerabilities to the Vulnerability Management team, and assisting with testing.
- Head of Human Resources: Responsible for ensuring that employee awareness and training programs are in place to educate employees about the Vulnerability Management Standard and their role in reducing the risk of vulnerabilities.
- External Legal Counsel: Responsible for advising the Vulnerability Management team on legal and regulatory requirements related to vulnerability management and response.

Each stakeholder listed above should be aware of their specific responsibilities related to the Vulnerability Management Standard and should ensure that they are fulfilled accordingly. In addition, roles and responsibilities should be regularly reviewed and updated to ensure that they remain accurate and effective.

9. Training and Awareness

All employees and stakeholders who are involved in managing vulnerabilities are required to be trained on the vulnerability management plan and their roles and responsibilities in executing it. This includes but is not limited to the following:

- Security awareness training: All employees are required to complete security awareness training that includes education on the importance of identifying and reporting vulnerabilities, as well as best practices for preventing them.
- Role-specific training: Employees who are directly involved in managing vulnerabilities, such as the Expresia Technical Lead, the Director of Infrastructure, and the Security Officer, will receive additional role-specific training on vulnerability scanning, remediation, and patch management.

- Awareness campaigns: Regular awareness campaigns will be conducted to remind employees of their role in managing vulnerabilities and to promote a culture of security throughout the organization.

In addition to the training, the vulnerability management plan will be regularly reviewed and updated to ensure that it remains current and effective.

10. Continuous Improvement

Expresia is committed to continuously improving our vulnerability management plan to ensure its ongoing effectiveness in mitigating security risks. To achieve this, we will regularly review and update the plan based on feedback, changes in our technology and business operations, and emerging threats and vulnerabilities.

The review process will include:

- Regular assessments of the effectiveness of vulnerability management controls and procedures, including vulnerability scanning, remediation, patch management, and configuration management.
- Analysis of incidents and vulnerabilities that were not previously identified, to identify gaps in our vulnerability management controls and procedures.
- Incorporation of feedback from employees, customers, and stakeholders on the effectiveness of the plan and the vulnerabilities that have been identified.
- Regular review of industry-standard frameworks and best practices to ensure that our vulnerability management plan remains up-to-date and effective.

Updates to the vulnerability management plan will be communicated to all relevant stakeholders, including employees, customers, and partners, and all necessary training and awareness programs will be conducted to ensure that everyone is aware of the changes and their roles in executing the plan.