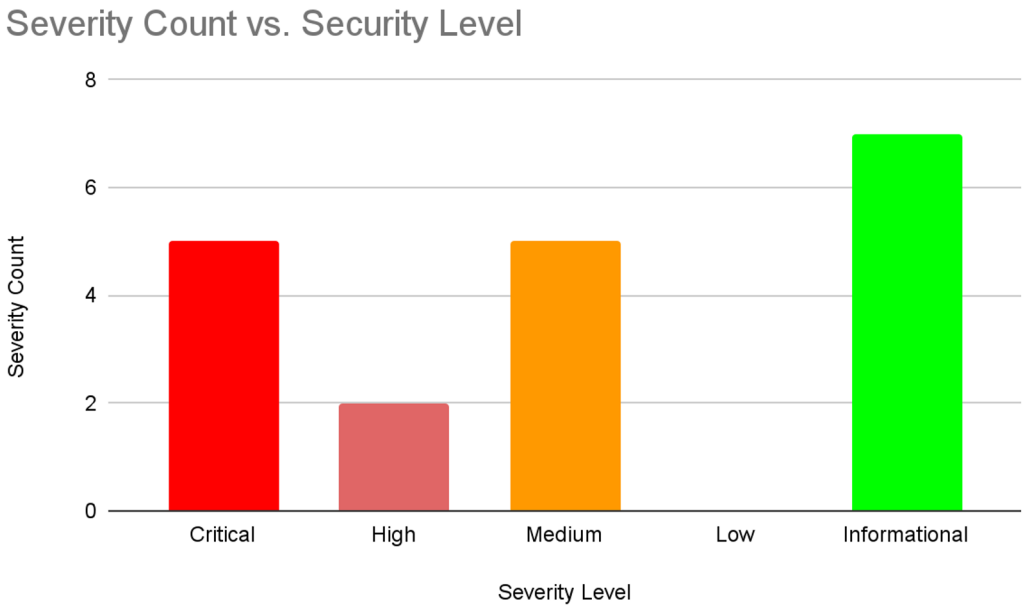
The Cozy Croissant Security Assessment

Finals-XX
January 14, 2023

Our Team

Summary of Findings



Jellyfin Default Admin Access

- **Summary**
  - Jellyfin admin account publicly accessible
  - Users can login as admin without authentication
- ***Business Impact***
  - Server shutdown
  - Compromise integrity of data

Recommendations

- Restrict the users access to only basic privilege
- Create a designated admin account with strong password

Rewards System Broken Access Control

- **Summary**
  - Source code publicly available
  - Users have admin rights by default
- ***Business Impact***
  - External access to company intellectual property
  - Sensitive customer information compromised

Recommendations

- Restrict access to source code
- Modify code to not give admin rights by default

SMB Users Using No Password

- **Summary**
  - Unauthorized access to system files
  - Some of users are admin
- ***Business Impact***
  - Workstations: Files can be stolen or changed
  - Kiosks: Display can be hacked

Recommendations

- Apply password policies
- Disable unused accounts
- Add inactive logout time

PCI DSS Compliance

Recommendations for Improvement

- Enforce strong password policies
  - Many accounts have no or weak password rules
- Assign user rights based off proper roles
  - Some normal users have administrator controls
- Encrypt sensitive information
  - Customer information are stored in clear text
- Securely develop custom software

Analysis

Positives

- Network Separation
- Input Validation
- Improved Security

Room For Improvement

- Misconfigured User Roles
- Password Policy
  - PCI Compliant password policies must be applied
- Cyber awareness
  - Ongoing cyber training

Questions?