Keanu Weblite Audit Response
“Pentest-Report Keanu Messaging UI & API 04.2021”

Summary

A Pentest and Audit was done of the beta Keanu and Web-lite platform in April 2021.

- One critical deployment configuration issue was found and immediately fixed.
- 4 medium issues were found and addressed in the next few weeks.
- 3 Low and 3 “Info” items were noted, with some being addressed, and others not relevant depending upon the deployed configuration.

The original report from Cure53.de can be found at https://keanu.im/docs/KNU-01-report.pdf

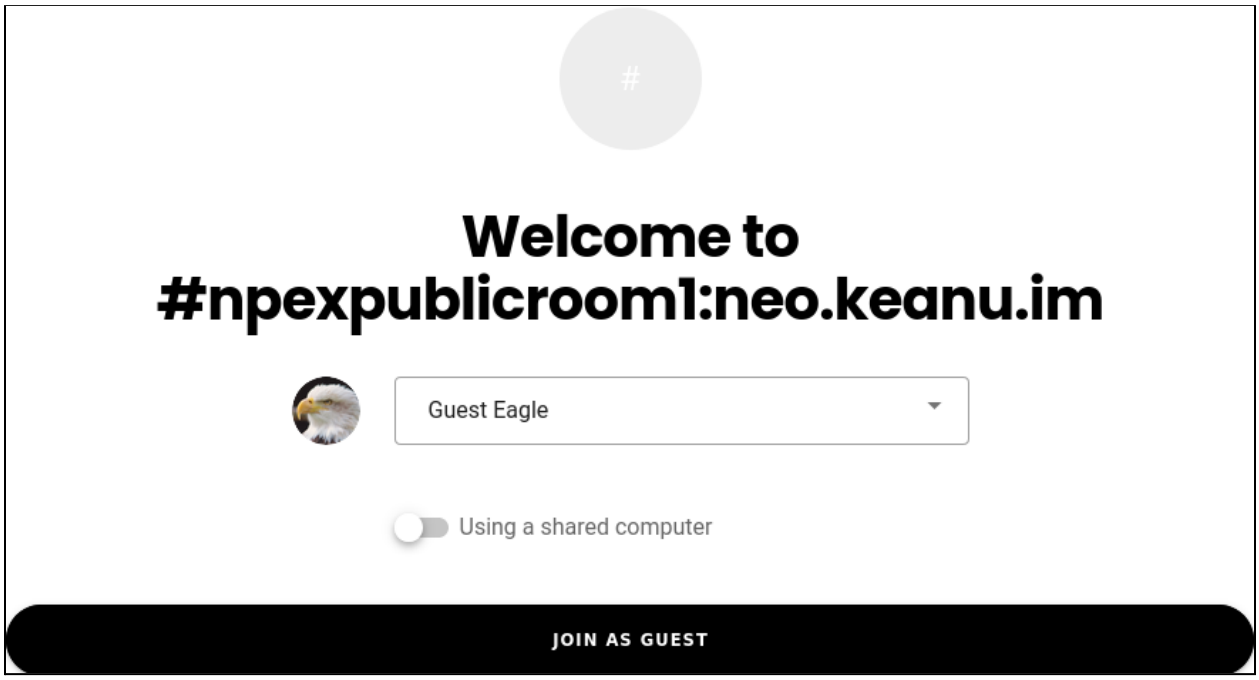
In the response to the identified vulnerabilities in this document, an issue will either be marked “fixed” if a change in core code or deployment scripts was the path to resolution or “addressed” if a configuration change was needed. All the issues and technical responses from the development team and third-party auditors are tracked publicly on issues here: https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues?sort=created_date&state=all

Identified Vulnerabilities

KNU-01-002 WP1: User-password and token persisted in localStorage (Low) - **FIXED VERIFIED DEC 2021**

https://gitlab.com/keanuapp/keanuapp-weblite/-/issues/120

- Implemented “Using a shared computer” toggle to disable use of localStorage



- We also have "LEAVE" prominently featured, which, if the user is only in one room, will also wipe their credentials from local storage if they are there.
- Lastly in the future, we will consider adding a PIN feature to encrypt credentials in local storage, and be required for physical access.

KNU-01-004 WP3: Insecure Jitsi Meet configuration allows participation (Medium) - Not “fixable”, but addressed in response below.

https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/8

“This weakness could be leveraged by adversaries to create new rooms. In effect, they could start using this service for free.” “It is recommended to protect easily guessable room names with a password.”

- The meet.keanu.im instance is meant as a public instance for anyone to use, just like meet.jit.si.
- We have active bandwidth usage monitors in-place to detect any unexpected increase in usage, so that we can throttle or shut it down.
- The use of "easily guessable room names without a password" is also done on process, for existing open-source projects that develop their work in the public. Other more private meetings use longer, nearly impossible to guest room codes, auto-generated by jitsi, as well as password protection.
- We also have deployed other instances of jitsi meet that only allow credentialed users to start new rooms/meetings.

KNU-01-005 WP2: Stored XSS via upload on MSIE (Low) - **ADDRESSED DEC 2021**

https://gitlab.com/keanuapp/keanuapp-weblite/-/issues/121

- All HTML and SVG content will be offered as download file only
- Add "Content-Disposition” header front to the Matrix Synapse home server.
- Do not allow use by old MSIE versions

KNU-01-006 WP3: Subdomain takeover via dead S3 bucket (Critical) - **FIX VERIFIED 2021**

Fix Note: This issue was fixed by the Guardian Project team during the testing phase and the fix was verified by Cure53.
https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/5

- Automated verification that regularly checks for incorrect entries to be implemented in monitoring infrastructure
- This issue was fixed by the Guardian Project team during the testing phase and the fix was verified by Cure53.

KNU-01-007 WP1,2: Missing X-Frame-Options permits Clickjacking (Medium) - **FIX VERIFIED DEC 2021**

https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/7

- Implement proper header via lambda for AWS deployment

KNU-01-008 WP2: SSRF related to missing allow-list on Federation server (Low) - **FIX VERIFIED DEC 2021**

https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/2

- implement a whitelist of known, trustworthy servers.

Miscellaneous Issues

KNU-01-001 WP1,2: General HTTP security headers missing (Medium) - **PROPERLY ADDRESSED DEC 2021**

https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/1

- Implement proper header via lambda for AWS deployment
- Addressed in new deployment automation, ready for testing at https://unready.im dev instance

KNU-01-003 WP2: Information disclosure via Gemfile artifacts (Info) - **PROPERLY ADDRESSED DEC 2021**

https://gitlab.com/guardianproject-ops/ops/-/issues/9
Moved to: https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/9

- In our gitlab ci deployment for the site, we now delete all Gemfile info: https://gitlab.com/keanuapp/letsconvene-www/-/blob/master/.gitlab-ci.yml#L24

KNU-01-009 WP3: Instance metadata enabled for EC2 instances (Medium) - **PROPERLY ADDRESSED DEC 2021**

https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/4

- Addressed in new deployment automation, ready for testing at https://unready.im dev instance

KNU-01-010 WP3: Missing logging and versioning for SSH key storage (Info) - **FIX VERIFIED DEC 2021**

https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/6

- Addressed in new deployment automation, ready for testing at https://unready.im dev instance

KNU-01-011 WP1/2: Cross-Origin-related HTTP security headers missing (Info) - **FIX VERIFIED DEC 2021**

https://gitlab.com/guardianproject-ops/keanu-audit-2021/-/issues/3

- Addressed in new deployment automation, ready for testing at https://unready.im dev instance