Coupa Security Assessment – CLMA

Executive Summary – R27

May 2020

Table of Contents

Observations Summary

Based on the manual vulnerability assessment and penetration testing performed, there were certain known security vulnerabilities found on the in-scope Web Applications. However, no sensitive data related to Coupa or its customers were exfiltrated.

Testing Team

The Coupa Internal security team and third-party vendor have carried out the assessment.

Testing Environment

The testing environment is hosted on the following URL.

https://clma-pentest.exaricontracts.com

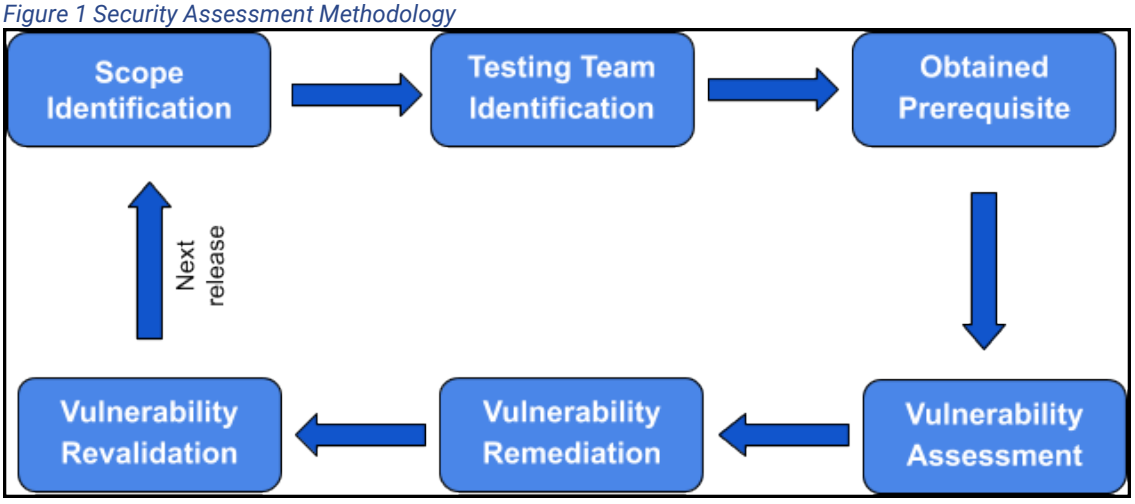
Assessment Dates

The 4-week assessment was performed from April 6, 2020 to May 01, 2020.

Coupa Security Assessment Methodology

The Coupa security team has developed a customized approach which is structured into six phases as described in Figure 1.

Figure 1 Security Assessment Methodology



Phase 1 – Scope Identification

Multiple stakeholders including, but not limited to, product managers and the security team schedule the annual security testing program. Depending on product criticality and the number of features developed, products are tested per release or on an on-demand basis.

Phase 2 – Testing Team Identification

Based on product criticality and testing team capacity, the testing team is chosen from one of the below options:

1. Internal Security Team
2. Crowdsourced Testers
3. Third Party Vendors

Phase 3 – Obtained Prerequisite

The phase includes gathering the information below from the respective development team:

- Understanding and walkthrough of the application
- Design documents
- In-scope product's URLs (Development environment)
- Different user roles

Note: Coupa uses the development environment for the security assessment and not the production environment.

Phase 4 – Vulnerability Assessment

This phase includes vulnerability identification, risk rating and JIRA ticket creation.

Vulnerability Identification

Coupa incorporates industry best practices to identify vulnerabilities which include the following methodologies:

- OSSTMM
- CREST
- OWASP
- PTES
- SANS
- NIST

These methodologies help ensure that the most recent and common web application vulnerabilities are identified in the most time and cost-efficient manners. However, testing varies based on the scope, timeline, nature of the application, and business logic flaws.

Common tested vulnerabilities include security misconfiguration, code injection, cross-site request forgery, cross-site scripting, insecure storage of sensitive data, authorization/authentication vulnerabilities, and business logic vulnerabilities, and more.

Risk Rating

After vulnerabilities are identified, a risk level is assigned to each finding.

Coupa evaluates risks by determining the likelihood and consequence of each vulnerability. An understanding of the nature of the vulnerability and its potential to affect technical and business objectives is developed by Coupa.

Additionally, Coupa evaluates vulnerabilities on the 4-level security scale which includes; Low, Medium, High, and Critical categories as described in Table 3 of Appendix 1.

Issue Tracker

For tracking, Coupa creates tickets which includes all observations and vulnerability details. Each vulnerability is tracked with a unique ID.

Phase 5 – Vulnerability Remediation

The Coupa Security Team prepares remediations plans for all issues found during penetration testing which are assigned to the appropriate development team.

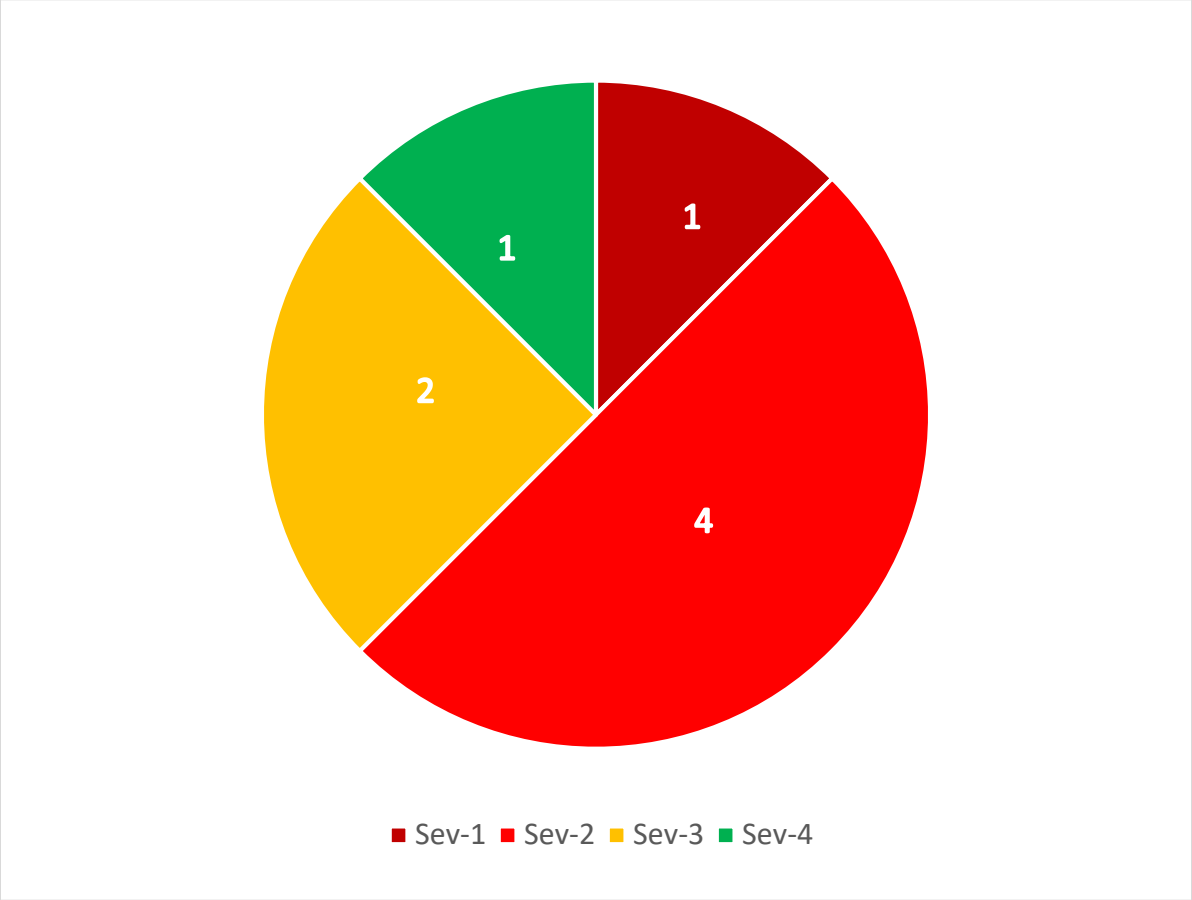
Phase 6 – Vulnerability Revalidation

After confirmation from the development team that an issue has been remediated, a retest on the updated environment is performed.

Vulnerability Summary

The chart displayed in Figure 2 gives the count of observations recorded during the execution of the assessment, along with the respective severity.

Figure 2 Vulnerability Severity and Count



Status of Findings

The post remediation assessment status is displayed in Table 2.

Table 1 Status of Findings

Sr. No.	Title	Severity	Status	Target Fixed Version	Module	Target Fixed Date DD/MM/YYYY	ID
1	CLMA Security: SSRF via Docx INCLUDETEXT fields and macros in .doc files	Critical	Fixed	clma27.0.1	CLMA	NA	CLMADV-12726
2	Stored XSS in Custom Configuration	High	Not Fixed	NA	CLMA	18/05/2020	CLMADV-12765
3	Stored XSS in Label and Site Header fields	High	Not Fixed	NA	CLMA	18/05/2020	CLMADV-12764
4	CLMA Security: PDF files returned via direct API call are missing no-cache header	High	Not Fixed	NA	CLMA	15/05/2020	CLMADV-12728
5	CLMA Security: Stored XSS via Adobesign status page	High	Fixed	clma27.5.0, clma27.0.1	CLMA	NA	CLMADV-12727
6	Content Security Policy (CSP) not implemented	Medium	Not Fixed	NA	CLMA	22/07/2020	CLMADV-12767
7	IDOR: A user who is not part of any CLMA groups can see the user-content data of CLMA user	Medium	Not Fixed	NA	CLMA	20/07/2020	CLMADV-12752
8	Information Disclosure through Exception Error	Low	Not Fixed	NA	CLMA	01/05/2021	CLMADV-12906

Appendix 1 – Vulnerability Evaluation

Coupa evaluates and ranks the vulnerability by determining the risk magnitude by the level of likelihood and consequence. Vulnerabilities are evaluated on a 4-level severity; Low, Medium, High, and Critical.

The likelihood and impact estimates are composed to calculate an overall severity for the risk. The is done by determining whether the likelihood is Low, Medium, or High. The same analysis is also performed for the impact.

The 0 to 10 scale is split into four sections as described in Table 3.

Table 2 Vulnerability Scale

Priority	Severity	CVSS Score	Description
1	**Sev 1 – Critical**	9 – 10.0	Vulnerabilities that affect all users of the platform, and/or affect the security of the platform or host system(s). Vulnerability is Critical that requires minimal or no technical skills and can easily be exploited with very minimal knowledge if discovered.
2	**Sev 2 – High**	7.0 – 8.9	Vulnerabilities that affect more than one user of the platform, and that require little or no user interaction to trigger. Vulnerability is High that requires little knowledge about the application and its workings and if discovered, an attacker can easily exploit the issue.
3	**Sev 3 – Medium**	4.0 – 6.9	Vulnerabilities that affect more than one user but may also require interaction or a specific configuration. Vulnerability is Medium that requires some scripting skills and familiarity of the application, it also depends on another security control which is currently implemented and if discovered needs some tools and manual techniques to exploit the issue.
4	**Sev 4 – Low**	0.1 – 3.9	Vulnerabilities that affect singular users and require interaction or significant prerequisites (MITM) to trigger. Also, leaking very basic information which might lead to information disclosure. Vulnerability is Low that is not exploitable and depends on multiple security controls that are in place and hence, cannot be exploited and is a best practice to have a multi layered security approach.

Appendix 2 – Coupa Security Assessment Tracker

The Coupa Security Assessment tracker for reported vulnerabilities is available from the following link:

Coupa Security Assessment Tracker - R27

Appendix 3 – References

- CVSS V3.1 specification document: https://www.first.org/cvss/specification-document
- OWASP testing guide: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- SANS Top 25: https://www.sans.org/top25-software-errors/
- WASC Threat Classification v2.0: http://projects.webappsec.org/w/page/13246978/Threat%20Classification