HR Acuity Penetration Test Remediation Plan

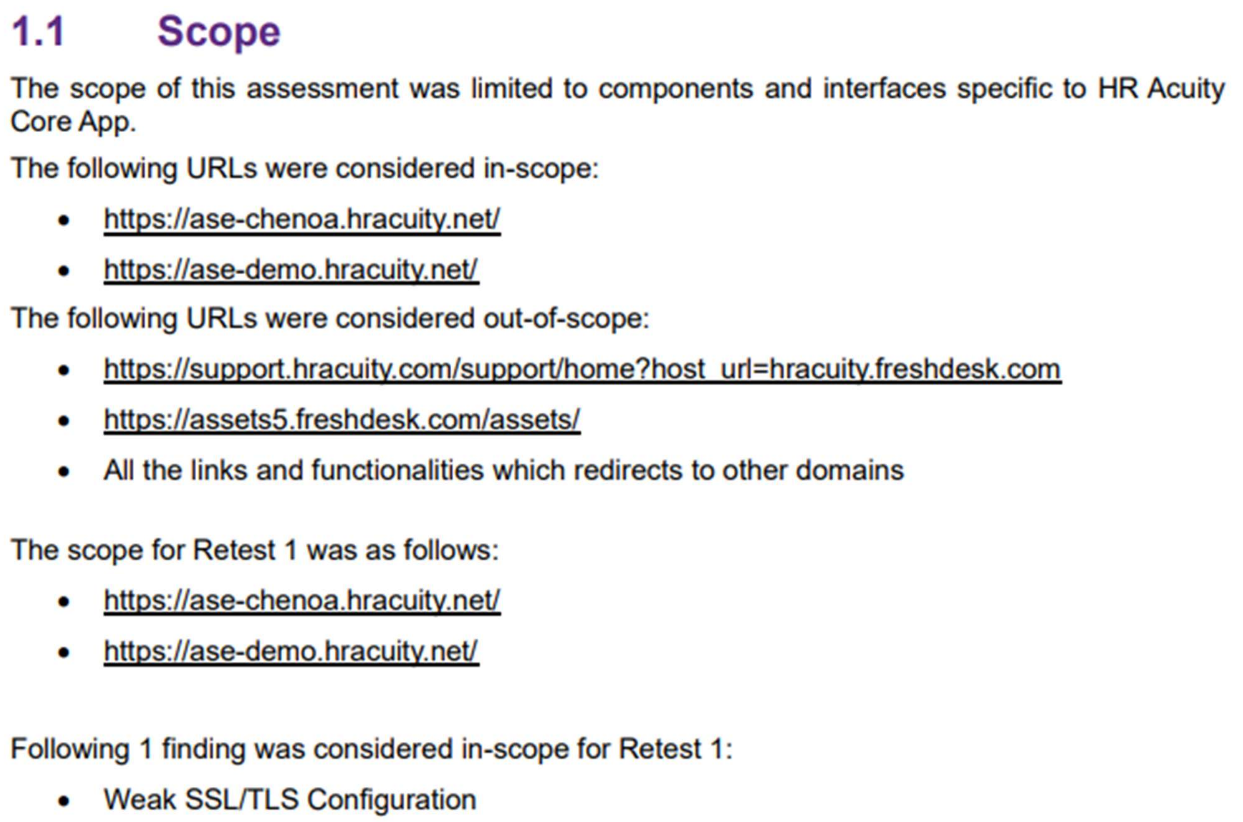
November 2021

During the assessment, Synopsys identified 1 finding characterized as follows:
• 1 Low vulnerabilities

Test Dates: 11/15/2021 – 11/23/2021

Retest Dates: 12/14/2021 – 12/15/2021

Scope:



1.1 Scope

The scope of this assessment was limited to components and interfaces specific to HR Acuity Core App.

The following URLs were considered in-scope:

- https://ase-chenoa.hracuity.net/
- https://ase-demo.hracuity.net/

The following URLs were considered out-of-scope:

- https://support.hracuity.com/support/home?host_url=hracuity.freshdesk.com
- https://assets5.freshdesk.com/assets/
- All the links and functionalities which redirects to other domains

The scope for Retest 1 was as follows:

- https://ase-chenoa.hracuity.net/
- https://ase-demo.hracuity.net/

Following 1 finding was considered in-scope for Retest 1:

- Weak SSL/TLS Configuration

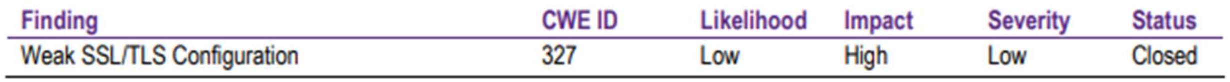
Vulnerability Matrix:

The vulnerability severity is determined using the likelihood and impact weights in the following table:

		Impact				
		Minimal	*Low*	*Medium*	*High*	*Critical*
Likelihood	*Critical*	Minimal	Low	Medium	High	Critical
	High	Minimal	Low	Medium	High	Critical
	Medium	Minimal	Low	Medium	Medium	High
	Low	Minimal	Low	Low	Low	Medium
	Minimal	Minimal	Minimal	Minimal	Low	Low

3 Findings

3.1 Summary of Findings



Finding	CWE ID	Likelihood	Impact	Severity	Status
Weak SSL/TLS Configuration	327	Low	High	Low	Closed

Remediation Plan:

Likelihood	Impact	Severity	Instance	Issue	HR Acuity Response	Status
Weak SSL/TLS Configuration						**FIXED AND VERIFIED**
Low	**High**	**Low**	**1**	The server-side SSL/TLS endpoint is configured to allow weak SSL/TLS cipher suites. These cipher suites have proven cryptographic flaws that can allow an attacker to decrypt or modify traffic.	Configuration will be updated to reject the weak SSL/TLS cipher suites.	Release Date: Q1 2022