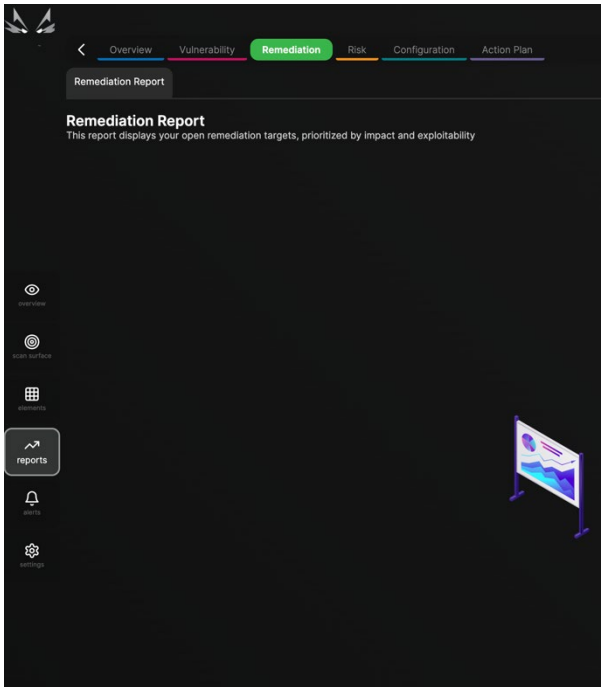
How To Guide – How to Remediate

This guide aims to assist you in starting the cyber vulnerability remediation process using the Insight portal. This tutorial assumes that you successfully managed to analyze the results of the Insight scans.

The vulnerability remediation process involves taking one of the following decisions as regards a detected vulnerability:

- Fix it by patching (often done as updating the vulnerable software)
- Fix it by decommissioning (removing the vulnerable software)
- Accept the risk of a vulnerability.
- Mark it as a False Positive.

The Insight Portal assists in the remediation process by tracking vulnerabilities and fixes, and by providing prioritized remediation plans. We recommend the following remediation flow:



1. Access and implement the remediation plan provided by the Insight Portal, following the next steps:

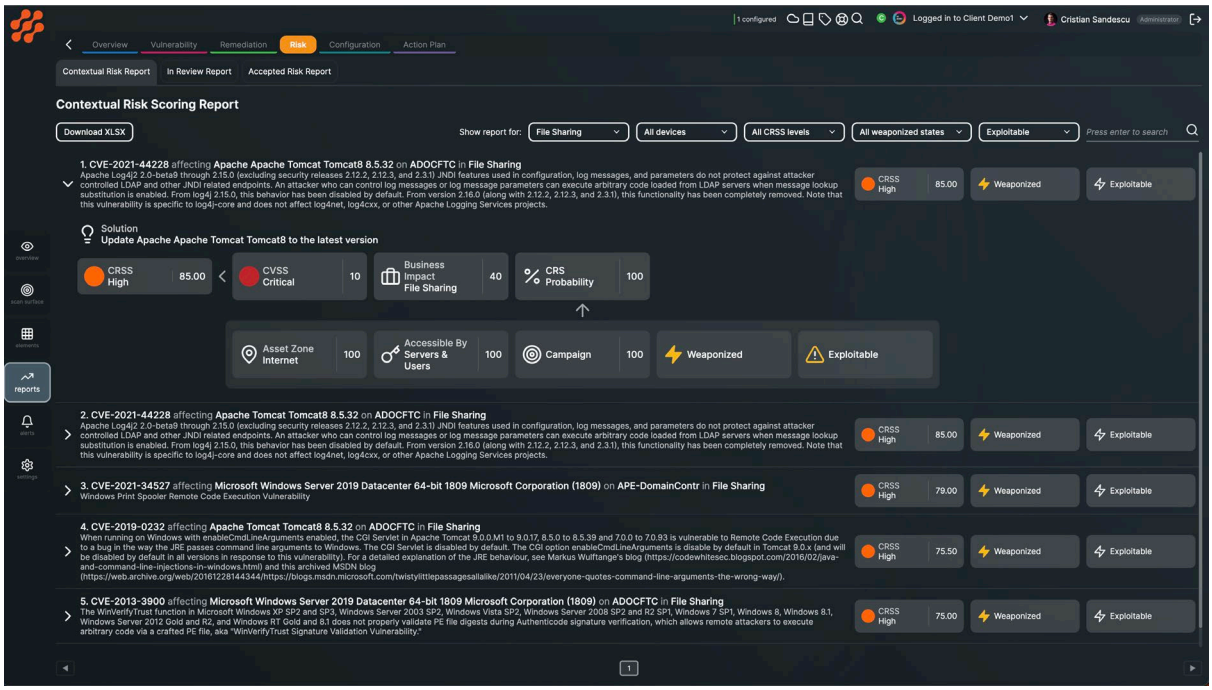
a. Access the *reports* menu. The menu is accessible from the options displayed on the left side of the screen.

b. Access the *Remediation Report sub-tab in the Remediation tab*. The tab and sub-tab are accessible from the options displayed on the top left side of the *reports* page.

c. Implement the recommended actions in the provided order.

The remediation actions are the best actions to take in order to reduce the largest amount of cybersecurity risk.

2. Remediate the riskiest vulnerabilities after taking the actions in the *Remediation Reports*. To achieve this:



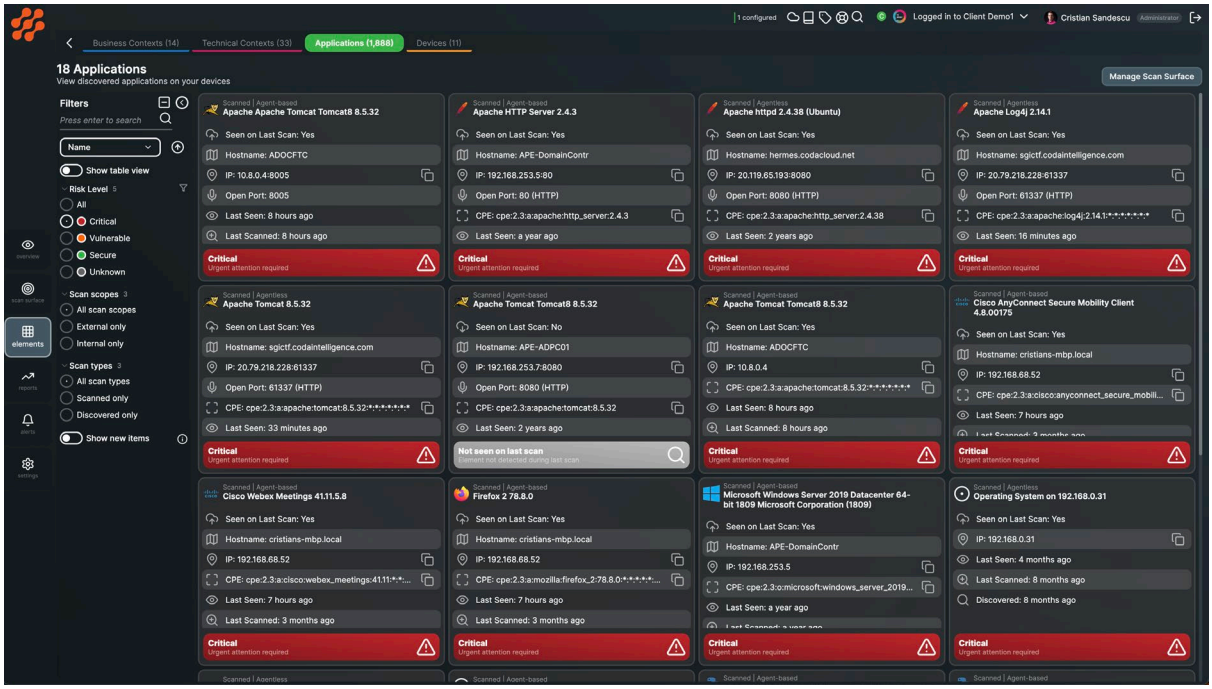
   a. Access the *reports* menu. The menu is accessible from the options displayed on the left side of the screen.

   b. Access the *Contextual Risk Report sub-tab from the Risk tab*. The tab and sub-tab are accessible from the options displayed on the top left side of the *reports* page.

   c. Click the dropdown placed in front of each CVE to read and implement the remediation action written in the *Solution* section.

   We recommend filtering vulnerabilities in the *Contextual Risk Report* by Criticality or by Weaponized level.

3. Remediate other critical vulnerabilities. To achieve this:



a. Access the *elements* menu. The menu is accessible from the options displayed on the left side of the screen.

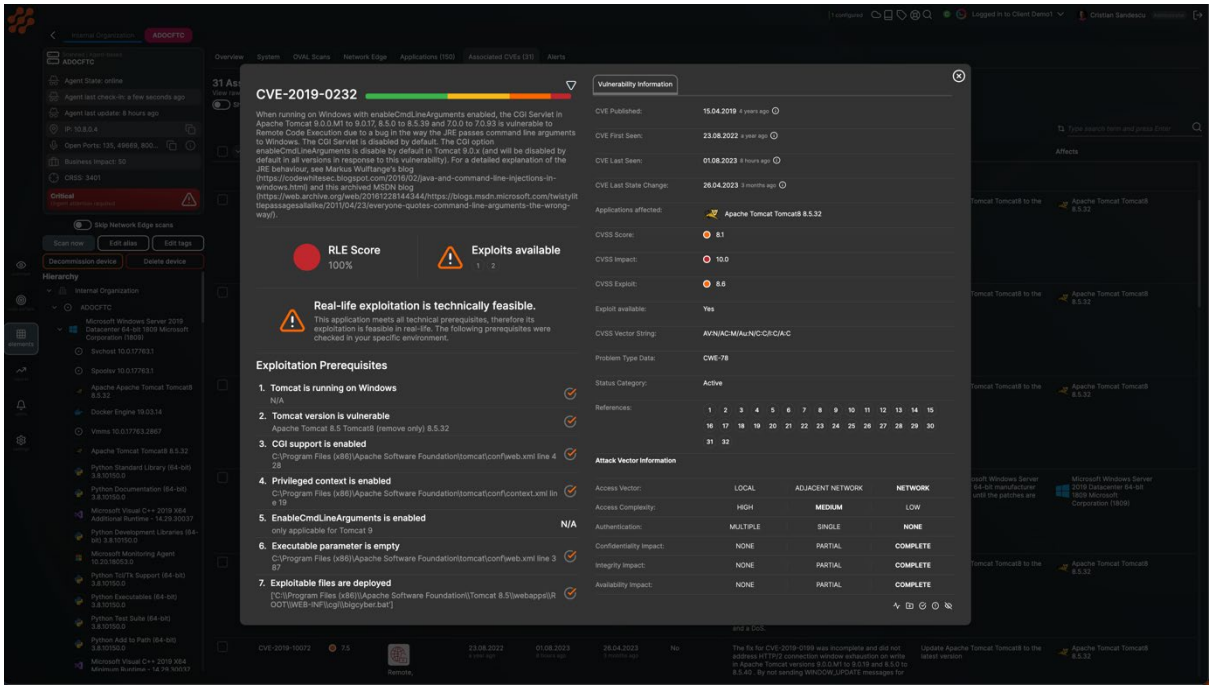
b. Choose to display the vulnerabilities by accessing the *Applications* tab. The tab is accessible from the options displayed on the top left side of the *elements* page.

   You can also access the *Devices* tab if you are interested to solve issues by device.

c. Filter by Criticality using the filters on the left side of the page.

d. Click an application and investigate the CVEs and the remediation actions using the table.

e. Click the CVEs. A pop-up will display. Use the buttons on the bottom right of the pop-up to:



i. Mark a vulnerability as active

ii. Add a vulnerability to review.

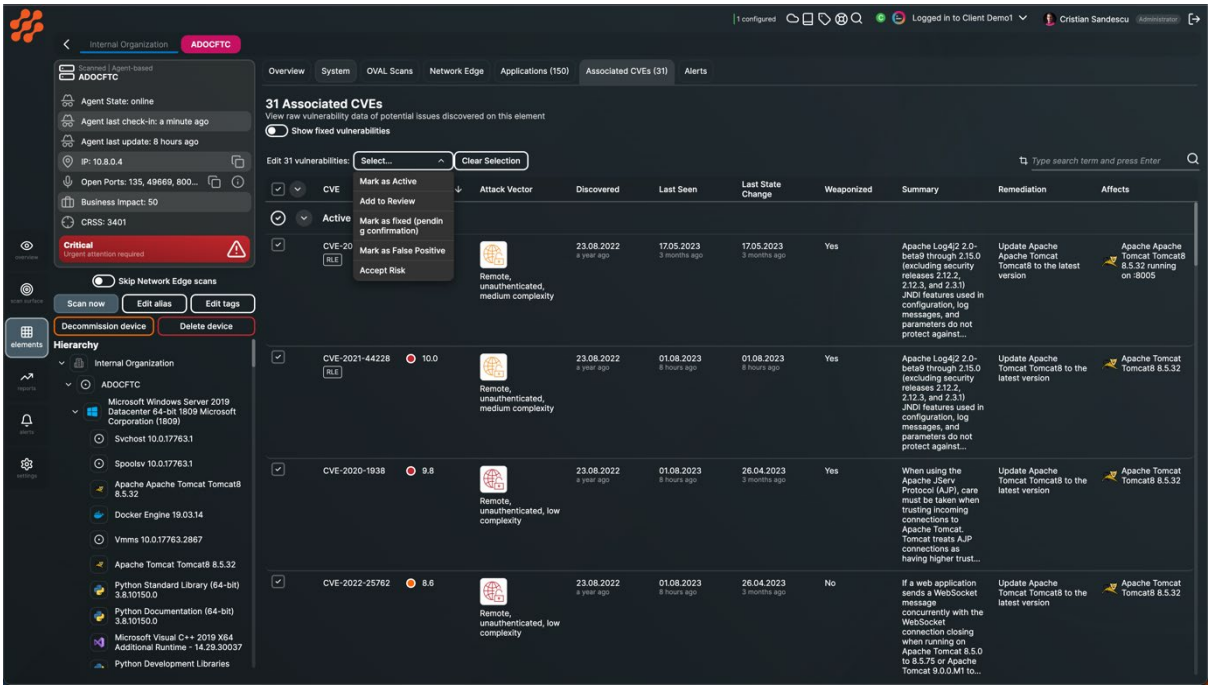
You can access vulnerabilities added to review using the *In Review Report* sub-tab from the *Risk* tab, accessible in the *reports* menu.

iii. Mark as fixed

Vulnerabilities marked as fixed are confirmed by the Insight portal at the next scan.

iv. Mark as a false positive

v. Accept the risk.



4. Track your remediation progress using the Remediation Tracking section in the *Customer Vulnerability Report*, accessible in the *reports* menu.