ciph0x01 Create CVE-2022-40084.md History

1 contributor

22 lines (12 sloc) | 743 Bytes

Affected Component

OpenCRX <=5.2.2 - https://github.com/opencrx/opencrx/

Description

OpenCRX before v5.2.2 was discovered to be vulnerable to password enumeration due to the difference in error messages received during a password reset which could enable an attacker to determine if a username, email or ID is valid.

Steps to reproduce

Navigate to password reset page on endpoint "/opencrx-core-CRX/RequestPasswordReset.jsp"

Enter an email, username or ID in the text field and click ok.

If the provided email, username or ID is valid the response will be "Password reset request successful for $username".

If it's not valid then the response will be "Unable to request password reset".

Impact

User enumeration.