

---

NCC Group  
XYZ Building  
2 Hardman Boulevard  
Spinningfields  
Manchester  
M3 3AQ  
<https://nccgroup.com>

September 23, 2022

Resco

Mlynske Nivy 5

82109 Bratislava

Slovakia

## Introduction

Between the days of February 14th and February 24th, 2022, two (2) consultants from NCC Group engaged in an IT Security Infrastructure Assessment for a total of thirteen (13) person-days of effort reviewing Resco's infrastructure.

The purpose of this assessment was to identify issues that could adversely affect the security of the IT infrastructure. This assessment was performed by NCC Group under the guidelines provided in the statement of work for the engagement.

Upon completion of the assessment, all findings were reported to Resco along with recommendations.

A follow-up validation exercise was performed between the dates of July 18th and July 21st, 2022 to validate whether originally reported issues had been addressed by Resco. This follow-up assessment established that the security posture was broadly appropriate to a solution of this type. A relatively small number of issues were identified and none were assessed to pose more than a medium risk.

## Detailed Letter of Engagement Overview

NCC Group is a global information assurance firm that specializes in application, mobile, network, host, and product security. Security conscious companies use NCC Group's Detailed Letters of Engagement to verify product attributes in view of current security best practices, standard security functionality, and product protection. More information about the Group's processes and products can be found at <https://nccgroup.com/>.

It is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This Detailed Letter of Engagement necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

## Testing Methods

Testing was performed using NCC Group's standard methodology for application and infrastructure assessments. Resco provided NCC Group with access to source code and documentation in order to improve the effectiveness of the testing. NCC Group's



---

consultants used a combination of manual test techniques and proprietary and public automated tools throughout the assessment. The following aspects were reviewed as part of this assessment:

- Configuration issues such as incorrect use of TLS when connecting to web servers
- Information leaks through exposed files, APIs, inappropriate error handling, and more
- Common web application vulnerabilities including Cross-Site Scripting, SQL Injection, and Cross-Site Request Forgery
- Authentication and authorization mechanisms
- Ability to obtain inappropriate access to sensitive and private information across users and tenants
- Business logic and ability to make unauthorized changes
- Privilege escalation from a normal user to higher-privileged roles
- Insecure storage of sensitive data

## Summary of Findings

After retesting efforts by NCC Group in accordance with the above methodology, the following issues remained open:

- Six (6) medium severity vulnerabilities
- Ten (10) low severity vulnerabilities
- Five (5) informational findings

© 2022 NCC Group

Prepared by NCC Group Security Services for Resco. Portions of this document and the templates used in its production are the property of NCC Group and cannot be copied (in full or in part) without NCC Group's permission. While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author (s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NCC Group's services does not guarantee the security of a system, or that computer intrusions will not occur.

