Executive Summary

This report presents the findings of the external infrastructure and unauthenticated web application security assessment conducted on behalf of Thomas International. The assessment was conducted between13/03/2023 and 14/03/2023.

Overview

The security posture of the systems within scope was found to be broadly appropriate to the assets which required protection. Nevertheless, a small number of issues were identified which should be addressed if the organisation's security model is to maintain an appropriate defence in depth basis. This illustrates the importance of ensuring that an otherwise robust security model cannot be undermined by isolated weaknesses.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
External Infrastructure Assessment	0	0	0	7	7
Web Application Assessment	0	0	1	1	2
Total	0	0	1	8	9

Assessment Summary

No significant risks were identified during the assessment of https://secure.thomasinternational.net. However, it was noted that the URL was protected by the Cloudflare Web Application Firewall (WAF); as such, a number of attempts to bypass or subvert the authentication mechanism were blocked. Whilst this can be considered best practice, should the Cloudflare WAF be accidentally reconfigured, or a bypass be published, it could leave the host exposed to attacks and vulnerable to issues that could not be tested during this assessment.

A large number of the URLs within scope were publicly accessible from the Internet. It is unclear from the scope as to whether this was expected, or whether this represents a gap in any intended inbound access control. However, it is believed that the former is the case. As such, an issue detailing the finding was raised as a medium risk to ensure inclusion in any organisational remediation procedures.

No significant risks were identified during the external infrastructure assessment, however several low risk issues were raised. Of note, the SSL/TLS implementation on a small number of hosts was not considered sufficiently cryptographically secure, and as such would not provide protection against brute-force decryption when compared to more modern cipher suites. A

clear text HTTP web service was also discovered, however no application was accessible at the time of the assessment. It is important to note that, should content be hosted on the service at a later date, or be hosted within a directory that wasn't accessible at the time of the assessment, the risk rating of this issue would be raised.

The remaining issues were all assessed to pose a low risk or are reported for information only. Nevertheless, it is recommended that these are reviewed and addressed so as to bring the systems within scope into line with security best practice. It is important to recognise that even low risk issues can be exploited in combination with other issues as part of a wider attack which seeks to compromise an environment or application. In addition, resolving lower risk issues can have the dual benefit of reducing the attractiveness of systems to opportunistic attackers as well as enhancing the overall security posture.

Strategic Recommendations

Although no significant risks were identified in this assessment, it is recommended that the issues outlined in this report are reviewed in line with a suitably robust defence in depth approach which continuously monitors the organisation's security posture.

It is recommended that consideration is given to performing an authenticated web application assessment. This will give greater level of assurance than it is possible to give as a result of a black box security assessment of this type.