thomas

Security Assessment

Executive Summary

This report presents the findings of the External Infrastructure and Web Application Security Assessment conducted on behalf of Thomas International UK. The assessment was conducted between 04/03/2024 and 05/03/2024.

The systems being assessed were a number of web applications and hosts belonging to Thomas International's online estate.

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	4	**4**
Web Application Assessment	0	1	0	2	**3**
Total	**0**	**1**	**0**	**6**	**7**

Assessment Summary

The assessment included an external access check for a number of web applications. The objective was to verify whether these applications were publicly accessible and if they were protected by the authentication portal. The review uncovered a number of accessible applications, in some cases hosting documentation and example scripts without authentication. An issue was raised so that Thomas International can review whether this is expected.

The authentication portal used by many of these applications was also reviewed for common vulnerabilities and avenues of attack. No significant threats were identified during this part of the assessment.

The infrastructure assessment uncovered similar issues to those raised during the previous iteration of this engagement. This included information disclosure in headers returned by some of the application servers, support for HTTP as well as HTTPS and minor SSL/TLS misconfigurations.

The domain name for the Dev Observability host was provided. When accessed via the FQDN, the site revealed a publicly exposed Grafana login portal. Depending on the business use case it may be beneficial to restrict access to known IP addresses. In addition, it was observed that it was possible to access the page directly via unencrypted HTTP. This could result in credentials being transmitted in clear text over the network.

While the majority of issues were all assessed to pose a low risk or are reported for information only, 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

It is recommended that the list of hosts flagged from the external access check is reviewed. Consideration should also be 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.

Although few 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.