Report for:

Security Assessment

Thomas International

February 2021

Version: 1.0

Executive **Summary**

This report presents the findings of the web application and external infrastructure security assessment conducted on behalf of Thomas International. The assessment was conducted between 12/02/2021 and 17/02/2021.

The systems under assessment were external facing hosts and applications that were publicly accessible and enabled users to access custom 'people assessments' conducted by Thomas International.

Overview

The assessment established that the security posture was broadly appropriate to an application of this type. A relatively small number of issues were identified and none were assessed to pose more than a medium risk. Nevertheless, it is recommended that these issues are reviewed and addressed in line with a robust defence in depth approach to security. In addition, addressing lower risk issues can have the added benefit of reducing a system's attractiveness to opportunistic attackers.

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):

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

Description	Critical	High	Medium	Low	Total
External Infrastructure Assessment	0	0	1	4	5
Web Application Assessment	0	0	1	8	9
Total	**0**	**0**	**2**	**12**	**14**

Assessment Summary

The most significant issue identified in the Web Application Assessment was the verbose error messages that were returned when erroneous data was provided as input. These verbose error messages returned stack trace information which could be used to gain a deeper understanding of the technologies of the web server. The error messages also returned version information about the .NET frameworks running on the systems, from this it was identified that the .NET version across multiple systems was outdated and had publicly disclosed vulnerabilities raised against it, this could put Thomas International at risk from a malicious user gaining unauthorised access to their internal network.

This finding was also identified as part of the External Infrastructure Assessment, and although the identified .NET version on one of the hosts was more up to date it could still provide another attack vector for a malicious user to gain access to Thomas International's internal network.

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 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

A proportion of the risk to which Thomas International was exposed was as a result of the use of outdated or unsupported software. It is therefore recommended that, in addition to addressing the individual issues which are set out in this report, the organisation's patching policy and procedures should also be reviewed to ensure that these issues do not recur once the individual instances documented here have been addressed.

Many of the identified issues were the result of hosts or systems which were not configured as securely as possible.

Some instances were observed in which default configurations were still in use and these configurations are rarely, if ever, the most secure. It is recommended that any remedial actions which are undertaken as a result of this assessment should also be reviewed for inclusion in the organisation's secure build standards and deployment procedures.

It is acknowledged that operational business requirements may mean that a risk has to be accepted (or partly accepted) rather than mitigated. Where this is the case, it is recommended that this is appropriately documented within the relevant Risk Register to ensure that the organisation maintains full visibility of the risk to which it is exposed.

It is recommended that the issues set out in this report should be addressed by a structured programme of remedial actions which are prioritised in accordance with the perceived risk to the organisation.