Report for:

External Infrastructure Security Assessment

Thomas International

May 2019

Version: 1.0

Prepared By: Adrian Villa

Email: Adrian.Villa@nccgroup.com

Telephone: +34 697184044

NCC Group PLC - Security Testing Audit and Compliance

XYZ Building,
2 Hardman Boulevard,
Spinningfields,
Manchester,
M3 3AQ
http://www.nccgroup.com

Executive Summary

This report presents the findings of the External Infrastructure Security Assessment conducted on behalf of Thomas InternationalThomas International. The assessment was conducted between 02/05/2019 and 03/05/2019 and was authorised by Thomas International.

Overview

The assessment established that the security posture was broadly appropriate to an infrastructure and web application of this type. A relatively small number of issues were identified; the most significant of which were identified in the External Infrastructure phase of the assessment and were assessed to pose a medium risk. Nevertheless, it is recommended that all issues are reviewed and addressed in line with a robust defence in depth approach to security.

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):

Phase	Description	Critical	High	Medium	Low	Total
1	External Infrastructure Assessment	0	0	4	4	**8**
2	Web Application Assessment	0	0	0	7	**7**
	Total	**0**	**0**	**4**	**11**	**15**

Assessment Summary

The most significant issue identified in the assessment was the presence of administrative interfaces exposed via unencrypted channels. One of the IP addresses assessed on the external infrastructure exposed a login form over unencrypted channels. This situation could allow a malicious attacker to intercept user credentials.

The web server hosting the application had verbose errors enabled. Consequently, sensitive information concerning the web server was disclosed which may be valuable to a malicious user for the purposes of developing further attacks.

The remote administration services exposed on the external infrastructure were not configured following security best practice and a number of issues were raised due to this situation.

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 environment 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.

More detailed information on each of the issues which were identified is included in Section 2 of this report.

Strategic Recommendations

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.

A large number of the identified issues were found to be 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.