Penetration testing highlight report

Restricted

Management Summary

Overview

NGS Secure (NGS) were contracted by the HCPC to conduct a security assessment consisting of an external penetration test of the HCPC IT infrastructure between 11 and 16 July 2016, the report was received in early August.

This forms part of the regular IT security testing regime that includes four infrastructure level and one application level tests per year. Testing is focused on vulnerabilities of the externally visible infrastructure and applications such as the corporate web site, the online register, online renewals portal and elements of the email service in the Microsoft Azure cloud.

NGS produce a detailed report identifying all vulnerabilities found and how they have been exploited. This highlight report is a management summary of that report's findings with the more sensitive and detailed information removed.

It is expected that each round of testing will identify new vulnerabilities as new security techniques are developed.

Approach

For this iteration of testing some perimeter protection devices were configured to allow NGS to bypass them. This is a test with some of our defences turned off and consequently is a worst case test scenario.

This test cycle included an Infrastructure security assessment as well as an application level assessment.

Key Findings

The results from this testing cycle were positive with no 'Critical' vulnerabilities. The testing identified an issue rated as 'important' that requires resolution in the short term; one issue rated as medium criticality that should be resolved as part of ongoing security maintenance and a small number of low criticality issues that should be addressed as part of routine maintenance tasks. The NGS conclusion was:

"… In general, the security posture of the external infrastructure as a whole could be improved in a number of ways."

Assessment method

NGS Secure classifies vulnerabilities into a number of categories using the Common Vulnerability Scoring System (CVSSv2) each having a relative risk associated with them. The table below describes the classification and shows the number of issues identified against each category within this testing cycle.

CVSSv2 Score	Category	Explanation	No. Issues Identified
9.0 - 10.0	Critical	Vulnerability was discovered that has been rated as critical and requires resolution as quickly as possible.	0
7.0 - 8.9	High	Vulnerability was discovered that has been rated as important and requires resolution in the short term.	1
4.0 - 6.9	Medium	Vulnerability was discovered that has been rated as of medium criticality and should be resolved as part of the on-going security maintenance of the system.	1
1.0 - 3.9	Low	Vulnerability was discovered that has been rated as of low criticality and should be addressed as part of routine maintenance tasks.	20
0 - 0.9	Info	A discovery was made that has been rated as of informational value which should be addressed in order to meet leading practice.	5
N/A	Good	Good security practices were being followed or an audit item was found to be present and correct.	1

Progress

The high and medium risk issues were addressed as a priority following the report. The Low risk and info issues have been addressed as part of ongoing maintenance and when project cycles allow. A number of Low risk issues will be delivered as part of the Web major project and one info issue cannot be mitigated.

Appendix A

There follows the management summary of the NCC report which has been redacted in order to remove exploit specific information that could aid someone in a malicious attack on the HCPC infrastructure. The full report is made up of 110 pages of technical specific information detailing how tests were executed and vulnerabilities identifies along with suggested mitigations where appropriate.

1 Management Summary

NCC Group is pleased to present the findings for the annual penetration testing security assessment conducted on behalf of Health and Care Professions Council (HCPC).

1.1 Overview and Scope

NCC Group was contracted by HCPC to conduct a security assessment of the external infrastructure and web applications, in order to identify security issues that in turn could negatively affect HCPC's business or reputation if they led to the compromise or abuse of systems.

This assessment was performed between 11/07/2016 and 16/07/2016, was carried out by [redacted], and was authorised by HCPC.

- External Infrastructure Assessment.
- Web Application Assessment

The IP addresses within the scope of this test are listed below:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

The web applications within scope are also listed below:

- edocs.hcpc-uk.org
- portal.hcpc-uk.org
- orfr.hcpc-uk.org
- www.hcpc-uk.org
- mrs.hcpc-uk.org
- gateway.hcpc-uk.org

1.2 Caveats

Due to the nature of the environment, checks that would have a high probability of causing disruption to the named hosts were excluded. Denial of service attempts were excluded for the same reasons.

1.3 Risk Ratings

The table below gives a key to the icons and symbols used throughout this report to provide a clear and concise risk scoring system.

It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

Symbol	Risk Rating	CVSSv2 Score	Explanation
	CRITICAL	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
	HIGH	7.0 - 8.9	A vulnerability was discovered that has been rated as important. This requires resolution in the short term.
	MEDIUM	4.0 - 6.9	A vulnerability was discovered that has been rated as of medium criticality. This should be resolved as part of the ongoing security maintenance of the system.
	LOW	1.0 - 3.9	A vulnerability was discovered that has been rated as of low criticality. This should be addressed as part of routine maintenance tasks.
	INFO	0 - 0.9	A discovery was made that has been rated as of informational value. This should be addressed in order to meet leading practice.
	N/A	N/A	Good security practices were being followed or an audit item was found to be present and correct.

1.4 Summary of Findings

A high risk issue was identified in the external infrastructure assessment relating to [redacted]. The HCPC application was found to make use of filters and web application firewall to sanitise user input[redacted]. To leverage this attack however they would need to trick a user into following a malicious link using a social engineering attack via email.

The key results found during the assessment can be summarised as follows:

[redacted].

[redacted].

Information Disclosure – Information was disclosed across the hosts assessed providing attackers with valuable information to target further attacks. Reducing the disclosure would improve the overall security posture of the external infrastructure.

Multiple SSL/TLS Issues – Multiple lower level SSL related issues were identified. Remediating these would help to ensure the confidentiality of application traffic.

ClickJacking Protection Enabled – A HTTP header preventing ClickJacking attacks was found to be set on the HCPC application mitigating the possibility of malicious users embedding the site within other sites. This is a common attack which an attacker uses to trick users into carry out actions on the site without them knowing

WAF / Filters Enabled – Input filters and a web application firewall were found to be enabled on the application. The protections stop common attack payloads by stripping out common tags in a blacklist and encoding user inputs.[redacted]

1.5 Conclusion

A high risk issue was identified within the external infrastructure assessment [redacted].

[redacted]. It is recommended that the above mentioned vulnerability is addressed accordingly as it may lead to a series of attacks, including phishing, page defacement or browser redirection to arbitrary Internet locations for malware delivery purposes.

The rest of the issues identified within the assessment were of low risk, these issues relate to the misconfiguration of network services and web servers which have either deployed weakened SSL services or disclose information that an attacker could leverage in future attacks. For example, the web servers disclose information about the underlying web technologies used to power the applications; similarly, the HCPC application also has a large amount of documents that contain large quantities of metadata. Upon extracting

said metadata, the consultant identified sensitive information such as usernames, network location. Combining all these information disclosure flaws an attacker could carry out a convincing social engineering attack with the information.

Another information disclosure vulnerability present in a number of the applications assessed was the ability to partially recover the filenames stored on the server. [redacted] Remedial changes should be applied to ensure that it is not possible to enumerate file names, additionally an investigation should be undertaken to ascertain [redacted]

In general, the security posture of the external infrastructure as a whole could be improved in a number of ways. [redacted] adjusting firewalls to prevent unnecessary responses from being sent and modifying the SSL configurations of the hosts would reduce the risk exposed and improve the security posture of the external infrastructure.

1.5.1 Next Steps

Short Term Actions

- [redacted]
- [redacted]

Medium Term Actions

- [redacted]
- [redacted]
- [redacted]
- [redacted].