



REPORT

# Innovate Healthcare Management Group

## Phase 1 Black Box Penetration Test

**Assessment Reference:** Innovate Healthcare Management Group\_2080903\_002  
**Issue Date:** 24 September 2018  
**Principal Consultant:** Will Gould

Executive Summary

ENGAGEMENT OVERVIEW

**Scope:** A unauthenticated, black-box penetration test of the website/portal.

**Date:** 20 September 2018 (1 man day)

**History:** This is the first technical assessment of the platform conducted by Cyberis.

SUMMARY

Cyberis performed a comprehensive black-box penetration test of the website/portal. Overall, the configuration of the remote host had a good level of security with no critical vulnerabilities identified.

The attack surface was minimal with port filtering implemented adequately. A single website was discovered, which only presented moderate to low risk issues.

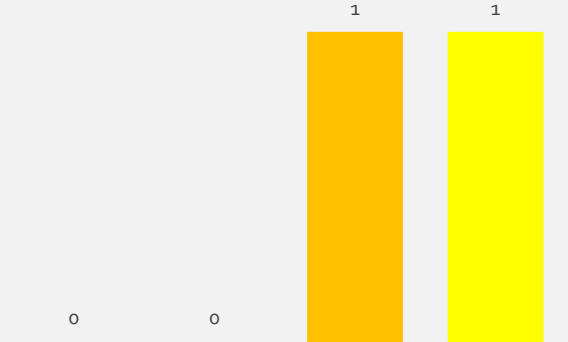
The website on the remote host was susceptible to several weaknesses in the configuration of encrypted services. These could lead to a suitably-positioned attacker gaining unauthorised access to sensitive information. Remediation is likely to be straightforward for the most part.

The website was also not configured with protective mechanisms which would help prevent man-in-the-middle attacks aimed at website users. Implementation of this protective mechanism is recommended to aid in the protection of encrypted connections.

Lower-risk issues identified in this report should be reviewed and remediated where appropriate.

RISK OVERVIEW

Number of risks by severity



| CRITICAL               | HIGH | MODERATE      | LOW    |
|------------------------|------|---------------|--------|
| 0                      | 0    | 1             | 1      |
| Treat risk immediately |      | Plan to treat | Review |

Business impact summary

|                               |   |
|-------------------------------|---|
| System Performance / Exposure |   |
| Privacy Violation             | X |
| Financial Damage              |   |
| Reputation Damage             |   |
| Non-Compliance                | X |

The risks identified during the assessment, if exploited, may have consequences for confidentiality, integrity and availability in the business areas indicated above.

Report Contents

Executive Summary.....2

Technical Summary.....4

Engagement Information .....9

    Classification and Handling .....9

    Version Control .....9

    Scope of Work.....9

    Information Provided .....9

    Constraints and Limitations.....9

    Logistics and Team Members .....9

Appendices.....10

    Appendix A.    SSL/TLS Multiple Implementation Weaknesses.....10

## Technical Summary

| REFERENCE                                      | I | E | RISK       | RECOMMENDATIONS  |
|--|---|---|------------|--|
| 1. SSL/TLS Multiple Implementation Weaknesses  | 4 | 3 | MODERATE   | Disable support for legacy SSL versions, and ensure all services are configured to accept connections made with strong ciphers only. |
| 2. HTTP Strict Transport Security Not Enforced | 3 | 2 | LOW        | Consider the implementation of HSTS to prevent unencrypted communications.   |
| 3. Password Autocompletion                     | 1 | 3 | NEGLIGIBLE | Set 'autocomplete=off' for all form fields collecting sensitive information, particularly login forms and password change forms.     |
| 4. Vulnerable Third-Party Script               | 1 | 1 | NEGLIGIBLE | Update the jQuery library to the latest version.   |

**Key:**

I = Impact

E = Exploitability

# 1. SSL/TLS Multiple Implementation Weaknesses

**MODERATE**

| DESCRIPTION   | RECOMMENDATIONS  |
|---|--|
| <p>Multiple weaknesses in the implementation and configuration of SSL services were identified during the engagement. The impact of these implementation weaknesses includes man-in-the-middle attacks or potentially information disclosure should connections be intercepted by a suitably-positioned attacker.</p>   | <p>Disable support for legacy SSL versions, and ensure all services are configured to accept connections made with strong ciphers only.</p>  |
| RISK DETAILS  | FURTHER INFORMATION  |
| <p><b>Affected Target(s)</b> <i>insight-portal.co.uk TCP Port 443</i></p> <p>There were several implementation weaknesses in the SSL/TLS service on the affected host. This included weak cipher suites and support for deprecated versions of SSL. The highest risk found was the support of SSL v3, which introduces a number of substantial weaknesses. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.</p> <p>It was also discovered that the remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.</p> <p>For a complete list of weaknesses and the services with which they were associated see <a href="#">Appendix A: SSL/TLS Multiple Implementation Weaknesses</a></p> | <p><b>External References:</b></p> <ul style="list-style-type: none"><li>• <a href="https://wiki.mozilla.org/Security/Server_Side_TLS">https://wiki.mozilla.org/Security/Server_Side_TLS</a></li></ul> |

## 2. HTTP Strict Transport Security Not Enforced

LOW

| DESCRIPTION  | RECOMMENDATIONS  |
|--|--|
| <p>The application is designed to operate exclusively over secure HTTPS channels, but HTTP Strict Transport Security (HSTS) has not been enabled.</p> <p>HSTS allows web servers to instruct supporting web browsers that application resources should exclusively be accessible over secure encrypted channels. It can protect against downgrade attacks and man-in-the-middle scenarios, and simplifies protection against cookie hijacking.</p> | <p>Consider the implementation of HSTS to prevent unencrypted communications.</p>  |
| RISK DETAILS   | FURTHER INFORMATION  |
| <p><b>Affected Target(s)</b> <i>insight-portal.co.uk TCP Port 443</i></p> <p>The application does not return Strict-Transport-Security headers to requesting browsers.</p>   | <p><b>External References:</b></p> <ul style="list-style-type: none"><li>• <a href="http://cwe.mitre.org/top25/#CWE-311">http://cwe.mitre.org/top25/#CWE-311</a></li><li>• <a href="https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure">https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure</a></li></ul> |

### 3. Password Autocompletion

NEGLIGIBLE

| DESCRIPTION   | RECOMMENDATIONS  |
|---|--|
| <p>Password input fields within the application were found to permit autocompletion, both when logging in to the application and when changing passwords</p> <p>Credentials remembered in this fashion will be cached on the user's workstation, within the Protected Storage area on Windows workstations. This information could be retrieved by an attacker with access to the user's workstation and used to compromise the account.</p>  | <p>Set 'autocomplete=off' for all form fields collecting sensitive information, particularly login forms and password change forms.</p>  |
| RISK DETAILS  | FURTHER INFORMATION  |
| <p><b>Affected Target(s)</b> <i>insight-portal.co.uk:443/</i></p> <p>The autocomplete attribute can be set on sensitive input fields, such as those containing passwords, to instruct the client web browser not to store these values locally. The attribute is not universally supported by modern web browsers, and will cause an application to fail strict XHTML validation, however.</p> <p>The password submission form in the login functionality did not have autocomplete disabled.</p> | <p><b>External References:</b></p> <ul style="list-style-type: none"><li><a href="https://cwe.mitre.org/data/definitions/522.html">https://cwe.mitre.org/data/definitions/522.html</a></li></ul> |

## 4. Vulnerable Third-Party Script

NEGLIGIBLE

| DESCRIPTION   | RECOMMENDATIONS  |
|---|--|
| The application uses out of date third party scripts which have known security issues.  | Update to the latest version of the jQuery library.  |
| RISK DETAILS  | FURTHER INFORMATION  |
| <p><b>Affected Target(s)</b> <i>insight-portal.co.uk:443</i></p> <p>Vulnerable script in use:</p> <ul style="list-style-type: none"><li>jQuery 1.8.2</li></ul> <p>The version of jQuery in use is vulnerable to a cross-site scripting attack. The function <code>jQuery(strInput)</code> does not differentiate selectors from HTML, giving attackers more flexibility when attempting to construct a malicious payload.</p> <p>A review of the application pre-authentication showed that the vulnerable function was not in use. Due to the nature of the assessment a full review of the use of the script post authentication was not conducted. This may be reviewed more fully during the upcoming application assessment. If it is found that the website does use the vulnerable function the risk would be increased.</p> <p>If the vulnerable feature is not used, the risk is negligible, however updating the script should be viewed as a remediation task to align with best practice.</p> | <p><b>External References:</b></p> <ul style="list-style-type: none"><li><a href="https://nvd.nist.gov/vuln/detail/CVE-2012-6708">https://nvd.nist.gov/vuln/detail/CVE-2012-6708</a></li></ul> |



## Engagement Information

### CLASSIFICATION AND HANDLING

This document is classified CLIENT CONFIDENTIAL and subject to the Cyberis Information Classification Policy and Information Handling Standard which are summarised below:

|                           |   |
|---------------------------|---|
| <b>Protective Marking</b> | Reports must be labelled according to their information classification.   |
| <b>Access</b>             | Access to reports and engagement data must be restricted to security cleared Cyberis consultants.                                 |
| <b>Storage</b>            | Electronic copies must be stored using an approved encryption algorithm/mechanism, such as 'PGP Zip'.                             |
| <b>Transmission</b>       | Electronic copies must be encrypted prior to transmission over the Internet, using an algorithm/mechanism approved by the client. |
| <b>Retention</b>          | Electronic copies must be retained according to requirements of the client if specified, or otherwise held indefinitely.          |
| <b>Destruction</b>        | Hard copies must be shredded. Electronic copies will be deleted using an approved overwrite method, such as 'shred'.              |

### VERSION CONTROL

| Date      | History | Author        | Comment             |
|-----------|---------|---------------|---------------------|
| 20 Sep 18 | 0.1     | Will Gould    | Initial Draft       |
| 20 Sep 18 | 0.2     | Gemma Moore   | Technical Review    |
| 24 Sep 18 | 0.3     | Will Gould    | Modifications       |
| 24 Sep 18 | 0.4     | Mark Crowther | Quality Review      |
| 24 Sep 18 | 0.5     | Will Gould    | Changes to findings |
| 24 Sep 18 | 1.0     | Mark Crowther | Approval and Issue  |

### SCOPE OF WORK

Innovate Healthcare Management Group (InnovateHMG) requires a penetration test of its main referral and case management portal. The application features multiple interfaces and user/account types, involving standard customer access, supplier/provider access and an admin portal for internal InnovateHMG colleagues.

The main portal is externally exposed to the Internet, used by customers and providers, supporting a hierarchy of user roles. It has approximately 25 – 30 pages with a small amount of functionality on each page.

Initially, InnovateHMG requires an unauthenticated, black-box penetration test of the website/portal as exposed to the Internet. This is to provide interim technical assurance that the portal does not expose the organisation to undue risk from vulnerabilities and weaknesses associated with the web server platform, portal and/or authentication mechanism by remote adversaries on the Internet.

In a second phase of testing, Cyberis will perform a comprehensive, authenticated Application Security Test according to its methodology (summarised in the next section) which has been reviewed and approved by industry bodies such as CREST and the National Cyber Security Centre (NCSC). This phase will assess the Internet exposed portal functionality available to all users of the systems to ensure access to data is adequately protected from unauthorised access to data and functionality by other users and adversaries without credentials.

### INFORMATION PROVIDED

The following information was provided to Cyberis at the commencement of the test:

- URLs of the hosts in scope:
  - [www.insight-portal.co.uk](http://www.insight-portal.co.uk)

### CONSTRAINTS AND LIMITATIONS

No constraints or limitation were encountered.

### LOGISTICS AND TEAM MEMBERS

All security testing was carried out at Cyberis' office, on the 20 September 2018 by:

- Will Gould (Consultant)

# Appendices

## APPENDIX A. SSL/TLS MULTIPLE IMPLEMENTATION WEAKNESSES

### SSL/TLS legacy Protocol Detection

The remote service accepts connections encrypted using SSL 3.0 and TLS 1.0. These versions of SSL and TLS are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.
- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

**Affected Host:**

- insight-portal.co.uk:443

**Recommendation:**

- Consult the application's documentation to disable SSL 3.0 and TLS 1.0.
- Use TLS 1.1 (with approved cipher suites) or higher instead.

### SSL Medium Strength Cipher Suites Supported

The remote host supports the use of SSL ciphers that offer medium strength encryption. Medium strength is identified as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

**Affected Host:**

- insight-portal.co.uk:443

**Details:**

|  |        |        |                    |          |
|--|--------|--------|--------------------|----------|
| Here is the list of medium strength SSL ciphers supported by the remote server : |        |        |                    |          |
| Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)                    |        |        |                    |          |
| DES-CBC3-SHA   | Kx=RSA | Au=RSA | Enc=3DES-CBC (168) | Mac=SHA1 |

Recommendation:

- Reconfigure the affected application if possible to avoid use of medium strength ciphers.

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Affected Host:

- insight-portal.co.uk:443

Details:

|  |        |        |               |          |
|--|--------|--------|---------------|----------|
| List of RC4 cipher suites supported by the remote server : |        |        |               |          |
| High Strength Ciphers (>= 112-bit key)                     |        |        |               |          |
| RC4-MD5  | Kx=RSA | Au=RSA | Enc=RC4 (128) | Mac=MD5  |
| RC4-SHA  | Kx=RSA | Au=RSA | Enc=RC4 (128) | Mac=SHA1 |

Recommendation:

- Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Affected Host:

- insight-portal.co.uk:443

**Recommendation:**

- Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

**END OF DOCUMENT**