



Penetration test report and response

This document describes RealVNC's response to a penetration test report conducted by an independent security agency, Falanx Cyber Defence

Version 1.0

RealVNC response to the report

Our customers' privacy is of paramount importance to RealVNC. As such, our flagship VNC Connect remote access software is built from the ground up with security and compliance in mind. We understand that our online infrastructure, website and the software itself must adhere to the highest security standards, and must remain ahead of the curve as active security threats emerge.

In March 2018, we contracted Falanx Cyber Defence (FCD), an independent security agency, to test our infrastructure and produce an objective penetration test report. FCD praised RealVNC's security as at a 'high level'. This document addresses the two potential issues uncovered in their report, which can be found appended to this document.

To learn more about VNC Connect security and compliance, visit our [dedicated security page](#). If you have any further questions, please do not hesitate to contact us at enquiries@realvnc.com or via realvnc.com/contact-us.

Web application password policy (medium risk)

The report identified our web application password policy as 'medium risk':

"The medium risk finding was related to the web application password policy that was in place. It was identified that the only control on a user's password was the length must be a minimum of 8 characters. No complexity rules or specific character combinations were enforced resulting in a password policy that would be susceptible to a brute force attack. This finding can be remediated by adhering to the advice provided in the findings section." (Page 5)

VNC Connect users must sign up for a RealVNC account online. This sign up process follows [NIST guidelines](#) rather than [OWASP guidelines](#). They are equally secure, but FCD favors the OWASP guidelines.

NIST guidelines make the password-creation process as user friendly as possible. Passwords must be at least eight characters long, but composition rules (having to include a combination of lower/upper case letters and numbers) are not required. NIST found that the supposed increase in complexity this affords is actually illusory ([research shows](#) that many people simply create an easy-to-guess password such as Pa55w*rd).

Providing a VNC Connect user follows our recommended password guidelines (not sharing the password with another online account or service), our NIST-based web application password policy is not a security threat. Note also we recommend that users turn on two factor authentication to protect against compromised or phished passwords.

Information disclosure (low risk)

The report identified the following as 'low risk':

"The low risk finding was related to several misconfigurations which resulted in information disclosure. A robots.txt file and a server version were exposed; both could allow an attacker to get a better idea of the applications structure and identify possible vulnerabilities related to the server details. This finding can be remediated by ensuring that all information externally available is reviewed for a business purpose and made as generic as possible." (Page 5)

Two potential problems are identified here:

- The robots.txt file is exposed
This file directs web crawling bots. Since this file contains no sensitive information or links to undocumented web pages, it has not been removed.
- The default apache file is exposed
This file has been removed (although in any case it did not contain sensitive information).



RealVNC's remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

Copyright © RealVNC Limited 2018. RealVNC and VNC are trademarks of RealVNC Limited and are protected by trademark registrations and/or pending trademark applications in the European Union, United States of America and other jurisdictions. Other trademarks are the property of their respective owners. Protected by UK patents 2481870, 2491657; US patents 8760366, 9137657; EU patent 2652951. 05Apr18

www.realvnc.com



RealVNC

RealVNC Penetration Test

COMMERCIAL IN CONFIDENCE

14/02/2018

1.0

Gordon Smith
Security Consultant

Contents

DOCUMENT CONTROL	3
Version History.....	3
EXECUTIVE SUMMARY	3
Objective.....	3
Background	3
Summary of Findings	4
Findings Analysis.....	5
Approach.....	6
Severity Level Description	7
Remediation Checklist	8
Application Penetration Testing.....	8
DETAILED FINDINGS – WEB APPLICATION.....	9
APP-M1 Weak Passwords Permitted	9
APP-L1 Information Disclosure	10

DOCUMENT CONTROL

Version History

Version	Date	Author	Comment
0.1	14/02/2018	Gordon Smith	Draft
0.2	19/02/2018	Joshua Higginbotham	QA (Technical)
0.3	19/02/2018	Gordon Smith	Updates
0.4	19/02/2018	Harry Lewis	QA (Non-Technical)
1.0	19/02/2018	Gordon Smith	Final report

EXECUTIVE SUMMARY

Objective

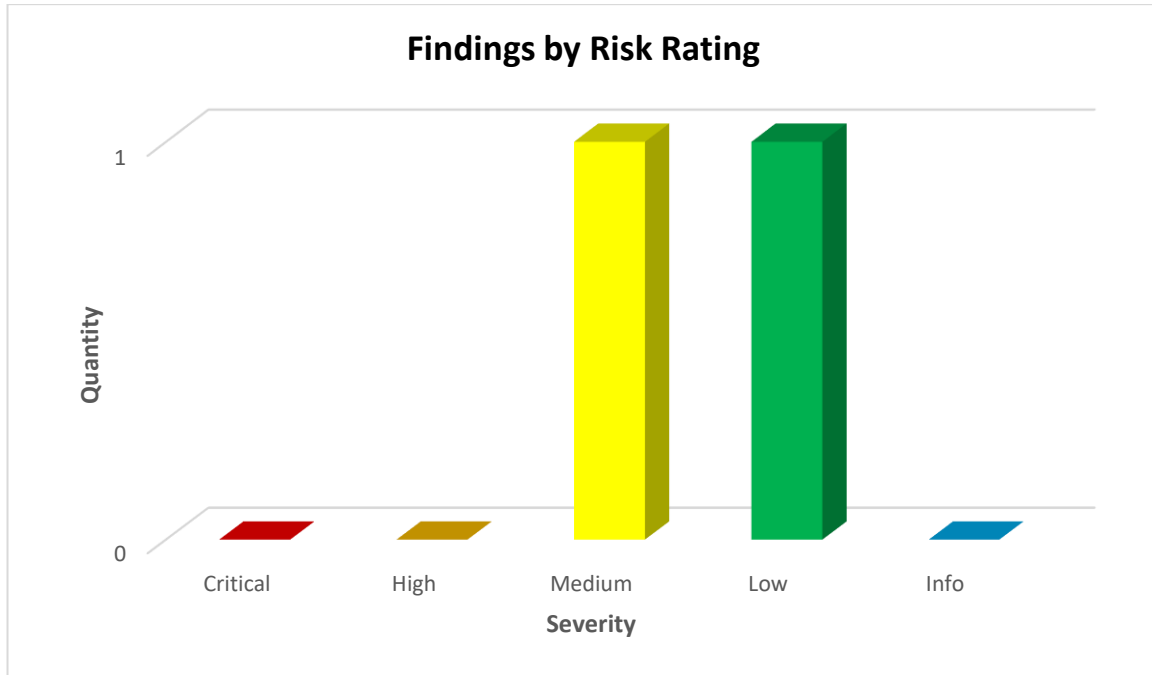
The client indicated that their objective in performing this engagement was to improve the security of the external facing services that they provide. The testing that was conducted should focus on identifying attack vectors in addition to the vulnerabilities and risks these attack vectors may expose.

Background

Falanx Cyber Defence ("FCD") has been engaged by RealVNC ("RealVNC") to perform a Security Assessment. The Security Assessment involves the following elements:

- Application Penetration Testing

Summary of Findings



Risk Rating	Findings
Critical	0
High	0
Medium	1
Low	1
Info	0

Findings Analysis

The penetration test identified 2 findings within the web application assessment. Of these findings one was rated at a medium risk rating, the other being a low risk rating.

The medium risk finding was related to the web application password policy that was in place. It was identified that the only control on a user's password was the length must be a minimum of 8 characters. No complexity rules or specific character combinations were enforced resulting in a password policy that would be susceptible to a brute force attack. This finding can be remediated by adhering to the advice provided in the findings section.

The low risk finding was related to several misconfigurations which resulted in information disclosure. A robots.txt file and a server version were exposed; both could allow an attacker to get a better idea of the applications structure and identify possible vulnerabilities related to the server details. This finding can be remediated by ensuring that all information externally available is reviewed for a business purpose and made as generic as possible.

Based on the issues and risk rating that were identified, RealVNC's security posture can be considered at a high level. RealVNC have taken a proactive approach to ensure they have reviewed their application against recent and trending flaws and have ensured adequate security controls are in place. To further increase the security posture, it is advised RealVNC follow the remedial advice highlighted in this report.

An external infrastructure assessment was also performed within the scope of this test; however, no issues were identified that could be quantified as a risk.

Approach

TEST TYPE	DATES	TARGETS
Web Application Assessment	1st February 2018 – 6th February 2018	manage.realvnc.com realvnc.help
External Infrastructure Assessment	1st February 2018 – 6th February 2018	212.119.29.130 212.119.29.131 212.119.29.132 212.119.29.177 212.119.29.178 212.119.29.179 165.254.191.194 165.254.191.195 165.254.191.196 165.254.191.229 165.254.191.230 165.254.191.231 165.254.191.245 165.254.191.246 165.254.191.247 165.254.239.130 165.254.239.131 165.254.239.132

Web Application Assessment

Falanx Cyber Defence conducted a web application assessment against the Internet Protocol (IP) addresses that were agreed in the scope and Testing Authorisation Letter (TAL). The web applications in scope were assessed in accordance with the OWASP Top 10 common vulnerabilities as well as our own testing methodology, aligned and approved by CREST.

Web applications are assessed with a combination of automated tools and manual exercises. All findings relating to any aspect of the web application have been manually reviewed. Although the network will have experienced increased network traffic, no intentional Denial of Service (DoS) attacks were carried out and Falanx Cyber Defence have configured the toolsets to minimise the network footprint.




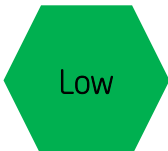

Consultant Contact Details

Gordon Smith
 gordon.smith@falanx.com
 07956 177 118

Client Contact Details

Andrew Woodhouse
Andrew.woodhouse@realvnc.com

Severity Level Description

Severity	CVSSv2 Score	Explanation
 Critical	9.0-10.0	Critical risk vulnerabilities will have a crippling effect on this service. Vulnerabilities of this level usually result in complete compromise of the affected host along with the possible network it resides on. In most instances, the exploit requires little to no knowledge and can be easily implemented.
 High	7.0-8.9	High risk vulnerabilities will be able to access potential sensitive information and cause denial of service (DOS) conditions. The severity is reduced as the issue is more difficult to exploit than that of a critical risk issue.
 Medium	4.0-6.9	Medium risk vulnerabilities will most often require further determination and technical ability to create a noticeable affect to an organisations business. In some cases, these issues require a high level of resourcing which can only be available by the likes of a funded project.
 Low	0.1-3.9	Low risk vulnerabilities have very little impact on an organisation's business. Exploitation of such vulnerabilities would either require local privileged access or to be used in combination to other findings.
 Info	0.0	These vulnerabilities do not possess a risk however they have been identified in the report for your information and awareness.

Remediation Checklist

This section lists the issues we identified accompanied with brief summarised details and remediation's.

Application Penetration Testing

Issue Number	Risk Rating	Issue Name	Host(s) Affected	Fixed
APP-M1	Medium	Weak Passwords Policy	https://manage.realvnc.com	<input type="checkbox"/>
APP-L1	Low	Information Disclosure	https://manage.realvnc.com	<input type="checkbox"/>

DETAILED FINDINGS - WEB APPLICATION



Medium

APP-M1 Weak Password Policy

CVSS: 4.0

Description

A weak password policy was identified being used on the web application. Weak passwords can be abused by attackers via a brute-force attack to gain unauthorised access to systems and data.

This creates a risk if an attacker were to obtain a valid password as they would be able to gain access to the underlying service and as such restricted information.

The password policy specified an 8 character password with no enforcing of special characters and combinations of upper and lower case characters.

This enabled the tester to change the password to the value password. The tester was also able to change the password back to the original password that was set that shows that no password history was in place.

Affected Host(s)

<https://manage.realvnc.com>

Remediation

It is recommended implementing a more complex password policy.

Password mechanisms should allow virtually any character the user can type to be part of their password, including the space character. Passwords should, be case sensitive in order to increase their complexity.

For Example:

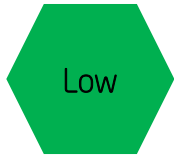
Password must meet at least 3 out of the following 4 complexity rules

- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (punctuation) – do not forget to treat space as special characters too
- at least 10 characters
- at most 128 characters
- not more than 2 identical characters in a row (e.g, 111 not allowed)

It is also recommended to ban common words such as, password.

References

https://www.owasp.org/index.php/Authentication_Cheat_Sheet#Implement_Proper_Password_Strength_Controls



APP-L1 Information Disclosure
CVSS: 2.0

Description

An information exposure is the intentional or unintentional disclosure of information to an actor that is not explicitly authorised to have access to that information. The information is either regarded as sensitive within the product's own functionality, such as a:

- private message; or
- provides information about the product or its environment that could be useful in an attack but is normally not available to the attacker, such as the installation path of a product that is remotely accessible.

There are many different types of problems that involve information exposures. Their severity can range widely depending on the type of information that is revealed.

The following pieces of information were identified during testing:

- Exposed robots.txt file – Found at the root of the application, this file can be useful in identifying files and folders that may not be normally accessible to users.
- Default Apache file – Found at /icons/README, this can provide an attacker with an indication of what software is in use.

Affected Host(s)

<https://manage.realvnc.com>

Remediation

Ensure that all systems only expose the minimum information that is required to deliver their business function.

References

<https://cwe.mitre.org/data/definitions/200.html>

PAGE INTENTIONALLY BLANK

This document contains commercial information provided in confidence to the recipient by Falanx Cyber Defence Limited. No part of this material may be reproduced or transmitted in any form or by any means, electronic, mechanical, photocopied, recorded or otherwise or stored in any retrieval system of any nature without the written permission of Falanx Cyber Defence Limited.

© Falanx Cyber Defence Limited 2018.

Falanx Cyber Defence Limited

A member of the Falanx Group

5 Kings House

1 Queen Street Place

London EC4R 1QS

United Kingdom

Tel. 00 44 (0) 20 7856 9450

E: info@falanx.com

www.falanx.com