

PENETRATION TEST REPORT AND RESPONSE

This document comprises the penetration test report conducted by an independent security agency, NCC Group, and RealVNC®'s response to it.

Version 2024.1
December 2024



RealVNC® response to the report

Our customers' security and privacy are of paramount importance to RealVNC®. As such, our flagship RealVNC® Connect remote access software is built from the ground up with security and privacy 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.

To maintain a level of assurance, in December 2024 we engaged NCC Group, an independent security agency, to conduct our annual penetration test – to test our infrastructure and produce an objective report. This document addresses any potential issues uncovered in their reports, which can be found appended to this document.

The scope for this test was the RealVNC® Connect Portal (including SSO, API access keys and purchase flows), CMS website and our On-Demand Assist website.

We believe this to be an exceptionally positive report with no critical, high or medium rated findings discovered. Although only Low and Informational, a number of the findings we don't believe to be exploitable or do not affect real-world usage. Additionally, we have a number of external mechanisms for prevention of abuse and active monitoring of our services via our 24/7 Security Operations Centre and Technical Operations team, which are not visible externally.

We are proud of the positive feedback received from NCC Group during the engagement and from the documented report. This penetration test is a baseline security review, something we conduct on an annual basis, but we believe companies should go above and beyond to prove their security to customers. This is why in addition to this yearly blackbox penetration test, we periodically engage with an additional external security specialist, Cure53, for full whitebox security audits of our services. To read more about that process, please see <https://www.realvnc.com/en/blog/cure53-security-audit-reaffirms-realvnc-strong-security-stance>.

We continuously monitor and assess both internal and external environmental changes, which may affect our security posture. To learn more about RealVNC® Connect security, visit our dedicated security page at <https://www.realvnc.com/en/connect/security/> and to learn about RealVNC®'s Information Security visit <https://trust.realvnc.com>.



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 2025. 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. 29 Jan2025



Real VNC Annual Web Application Security Assessment

Real VNC

Version 1.0 – December 19, 2024

1 Executive Summary

This report presents the findings of the Real VNC Annual Web Application Security Assessment conducted on behalf of Real VNC. The assessment was conducted between 09/12/2024 and 12/12/2024.

The CMS system being assessed allowed users to view Real VNC's product portfolio.

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 low risk. Nevertheless, it is recommended that these 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 component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
CMS Website	0	0	0	0	0
Real VNC Portal	0	0	0	2	2
Real VNC Portal and ODA Branding Site	0	0	0	0	0
Real VNC Portal, CMS Website and ODA Branding Site	0	0	0	1	1
Total	0	0	0	3	3

Assessment Summary

The most significant issues identified in the web application assessment were that sessions were not invalidated until approximately 5 minutes after a password change. This creates a security risk by allowing an attacker, who may have already hijacked a session, to continue accessing the application even after the legitimate user changed their password. Additionally, the use of excessively long expiry times for JSON Web Tokens (JWTs) in password reset and email invitation links increases the likelihood of token misuse. If an attacker intercepts or obtains a token, they could exploit it before its expiration to gain unauthorised access. Lastly, the absence of DNS Security Extensions (DNSSEC) leaves the application vulnerable to DNS spoofing attacks, which could redirect users to malicious sites or compromise sensitive data. Addressing these issues is essential to enhancing the overall security of the application.

The remaining issues were all assessed as reported for information only. Nevertheless, it is recommended that these are reviewed and addressed so as to bring the Real VNC web applications 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 the [Finding Details](#) section of this report.

Strategic Recommendations

To mitigate the risk posed by sessions not being invalidated until approximately 5 minutes after a password change, it is recommended to implement session management mechanisms that immediately invalidate all active sessions when a user changes their password. This includes revoking any existing session tokens and requiring users to log in



again across all devices. This measure will ensure that any potential unauthorised access resulting from a compromised session is immediately terminated.

For addressing the excessive expiry times of JSON Web Tokens (JWTs) in password reset and email invitation links, it is advisable to reduce the token validity period to a minimal, reasonable duration, such as 15–30 minutes. This will minimise the window of opportunity for an attacker to exploit the token.

To enhance DNS security, it is recommended to enable and configure DNS Security Extensions (DNSSEC) for all relevant domains. DNSSEC ensures the authenticity and integrity of DNS responses by digitally signing them, thereby protecting users from DNS spoofing and man-in-the-middle attacks. Implementing DNSSEC will help safeguard users and the application from potential redirection to malicious servers.

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.

2 Table of Contents

1	Executive Summary	2
1.1	Overview	2
1.2	Assessment Summary	2
1.3	Strategic Recommendations	2
2	Table of Contents	4
3	Document Control	5
3.1	Client Confidentiality	5
3.2	Proprietary Information	5
4	Technical Summary	6
4.1	Scope	6
4.2	Caveats	6
4.3	Post Assessment Cleanup	6
5	Table of Findings	7
6	Risk Ratings	8
7	Finding Details	10
8	Contact Info	25



3 Document Control

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Real VNC.

NCC Group gives permission to copy this report for the purposes of disseminating information within your organisation or any regulatory agency.

Document Data

Data Classification	Client Confidential
Client Name	Real VNC
Project Reference	E019128
Proposal Reference	O-219331
Document Title	Real VNC Annual Web Application Security Assessment
Author	Dakila Samatra

Document History

Version	Issue Date	Issued by	Change Description
0.1	2024-12-09	Dakila Samatra	Draft for NCC Group internal review only
0.2	2024-12-13	Robert Ray	Revised QA
1.0			Released to client
1.1		Daki Samatra	Removed Default Pages Present and changed Session Not Invalidated upon Change of Password to Session Invalidation Delay: Up to 5 Minutes After Password Change from the Finding Details section

Document Distribution List

Name	Role
Andrew Woodhouse	Chief Information Office
Benjamin May	Head of Cyber Security



4 Technical Summary

NCC Group was contracted by Real VNC to conduct a security assessment of the systems within scope in order to identify security issues that could negatively affect Real VNC's business or reputation if they led to the compromise or abuse of systems.

Scope

The security assessment was carried out in the staging environment and included the following section. The assets within the scope are listed below:

Web Application Assessment

- CMS: <https://stage-www.realvnc.com>
- RealVNC Portal: <https://s-manage.realvnc.com>
- ODA Branding Site: <https://s-www.realvnc.help>

Caveats

It was discussed and agreed upon that although an admin page was discovered on the CMS it is worth noting that the application was protected by the Cloudflare WAF (Web Application Firewall) which limits external access, in which NCC group was whitelisted for testing purposes. Testing access for portal access was not part of the scope in this engagement.

The SSO account pentest-technician@betjbot.onmicrosoft.com was inaccessible during the course of the security assessment and, as a result, could not be tested.

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 reason.



5 Table of Findings

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors.

Title	Status	ID	Risk
Session Invalidation Delay: Up to 5 Minutes After Password Change	New	RQ9	Low
JWT Expiry Excessive in Password Reset and Email invitation Links	New	KY2	Low
DNS Security Extension (DNSSEC) Not in Use	New	QUR	Low
Weak Password Complexity Requirements	New	2QK	Info
Outdated WordPress Plugin	New	HET	Info
Users Can Reuse Old Passwords	New	ETJ	Info
Wildcard TLS Certificate in Use	New	GYT	Info
Username Enumeration	New	NE6	Info
Misconfigured Content Security Policy	New	DFC	Info



6 Risk Ratings

The table below gives a key to the ratings 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.

Risk Rating	CVSS 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 high. This requires resolution in the short term.
Medium	4.0 - 6.9	A vulnerability was discovered that has been rated as medium. 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 low. This should be addressed as part of routine maintenance tasks.
Info	0 - 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.

Impact

Impact reflects the effects that successful exploitation has upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

Rating	Description
High	Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.
Medium	Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.
Low	Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.



Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

Rating	Description
High	Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.
Medium	Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.
Low	Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.



7 Finding Details

Low

Session Invalidation Delay: Up to 5 Minutes After Password Change

Overall Risk Low

Impact Low

Exploitability Low

Finding ID NCC-E019128-RQ9

Component Real VNC Portal

Category Session Management

Status New

Description

The Real VNC Portal web application experiences a delay of up to 5 minutes in invalidating the currently logged-in session after a password change. This delay can allow a potentially compromised account to remain logged in, giving an attacker continued access to the account during this period.

```
POST /en/auth/reset_password HTTP/1.1
Host: s-manage.realvnc.com
```

The previous session was invalidated approximately 5 minutes after the password reset:

```
GET /en/ HTTP/1.1
Host: s-manage.realvnc.com
Cookie: session=<SESSION_TOKEN>
```

```
HTTP/1.1 401 Unauthorized
Server: Apache
Content-Length: 9470
```

Recommendation

Configure the web application to immediately invalidate the current session upon a password change and log the user out. This will ensure that any malicious users who are concurrently logged in are automatically logged out, mitigating the risk of continued unauthorised access.¹

Location

- <https://s-manage.realvnc.com/en/>

1. OWASP Session Management: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#renew-the-session-id-after-any-privilege-level-change



JWT Expiry Excessive in Password Reset and Email invitation Links

Overall Risk Low

Impact Medium

Exploitability Low

Finding ID NCC-E019128-KY2

Component Real VNC Portal

Category Session Management

Status New

Description

The JSON web tokens (JWTs) for the Real VNC Portal Password reset and Email invitations were set with an expiry time that was excessive. This increases the risk that tokens stolen by, or inadvertently disclosed to, malicious actors can be used to gain unauthorised access.

As the validity of a JWT is generally not revoked on demand but relies on the expiry time which is set as a built-in property of the token, a relatively short time frame is recommended. For example, a JWT was set with a payload that included the following 'issued at' and 'expires at' parameters:

Email Invitation:

"iat": 1733917260 11/12/2024 11:41:00 UTC

"exp": 1736509260 10/01/2025 11:41:00 UTC

The difference between these timestamps shows that the token was valid for 30 days.

Password Reset:

"iat": 1733918146 11/12/2024 11:55:46 UTC

"exp": 1734004546 12/12/2024 11:55:46 UTC

The difference between these timestamps shows that the token was valid for 1 day.

Recommendation

Set the expiry period of the JWT to as short a period as possible, appropriate to the use case.² For example, services with sensitive data and functionality typically have session timeouts of around 20 minutes. Context is also a factor: a validity period of an hour would be appropriate for web service consumers outside a browser environment - that is, server-to-server. If necessary, use a token refresh mechanism to extend access when a token approaches expiry.

Location

- https://s-manage.realvnc.com/en/profile/accept_invitation?token=
- https://s-manage.realvnc.com/en/auth/reset_password?token=

2. RFC – JSON Web Token (JWT) – Registered Claim Names: <https://tools.ietf.org/html/rfc7519#section-4.1>



DNS Security Extension (DNSSEC) Not in Use

Overall Risk Low

Impact Medium

Exploitability Low

Finding ID NCC-E019128-QUR

Component Real VNC Portal, CMS Website and ODA Branding Site

Category Configuration

Status New

Description

The `stage-www.realvnc.com`, `s-manage.realvnc.com`, and `s-www.realvnc.help` domains did not make use of DNS Security Extension (DNSSEC). DNSSEC is a set of security extensions to DNS that provides a means for authenticating DNS records. DNSSEC is designed to protect applications from using forged DNS data created by DNS cache poisoning.

Domain Name: <code>s-manage.realvnc.com</code>	
Analyzing DNSSEC problems for <code>s-manage.realvnc.com</code>	
.	<ul style="list-style-type: none"> Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
com	<ul style="list-style-type: none"> Found 1 DS records for com in the . zone DS=19718/SHA-256 has algorithm ECDSAP256SHA256 Found 1 RRSIGs over DS RRset RRSIG=61050 and DNSKEY=61050 verifies the DS RRset Found 2 DNSKEY records for com DS=19718/SHA-256 verifies DNSKEY=19718/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19718 and DNSKEY=19718/SEP verifies the DNSKEY RRset
realvnc.com	<ul style="list-style-type: none"> No DS records found for realvnc.com in the com zone No DNSKEY records found ns-1853.awsdns-39.co.uk is authoritative for s-manage.realvnc.com s-manage.realvnc.com A RR has value 146.101.60.65 No RRSIGs found

Figure 1: DNSSEC not in use for the `s-manage.realvnc.com` domain

All answers from a DNSSEC protected zone will be digitally signed. By verifying the digital signature, the DNS resolver can confirm that the information is identical to the information published by the zone owner and served on an authoritative DNS server.

Recommendation

It is recommended that DNSSEC should be implemented on the `stage-www.realvnc.com`, `s-manage.realvnc.com`, and `s-www.realvnc.help` domains. Consult with your registrar on how this can be performed.^{3 4}

3. DNSSEC: <https://technet.microsoft.com/en-us/library/jj200221.aspx>, <https://www.dnssec.net/>

Location

- stage-www.realvnc.com
- s-manage.realvnc.com
- s-www.realvnc.help



Weak Password Complexity Requirements

Overall Risk Informational

Impact Low

Exploitability Low

Finding ID NCC-E019128-2QK

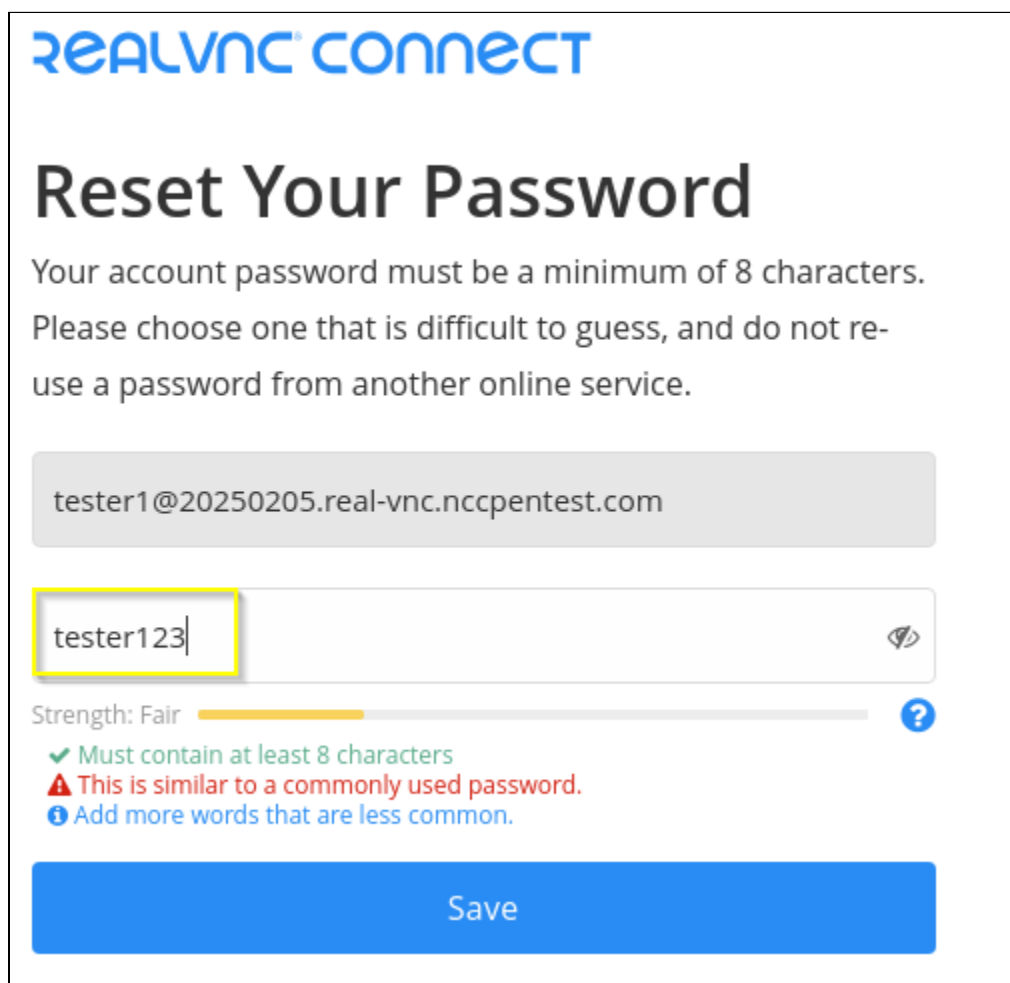
Component Real VNC Portal

Category Authentication

Status New

Description

The Real VNC portal web application enforced the following weak restrictions on users passwords. An attacker may guess or brute-force weak user passwords, especially in the event of a password database breach.



REALVNC® CONNECT

Reset Your Password

Your account password must be a minimum of 8 characters.
Please choose one that is difficult to guess, and do not re-use a password from another online service.

tester1@20250205.real-vnc.nccpentest.com

tester123

Strength: Fair

- ✓ Must contain at least 8 characters
- ⚠ This is similar to a commonly used password.
- ℹ Add more words that are less common.

Save

Figure 2: Setting a weak complexity password

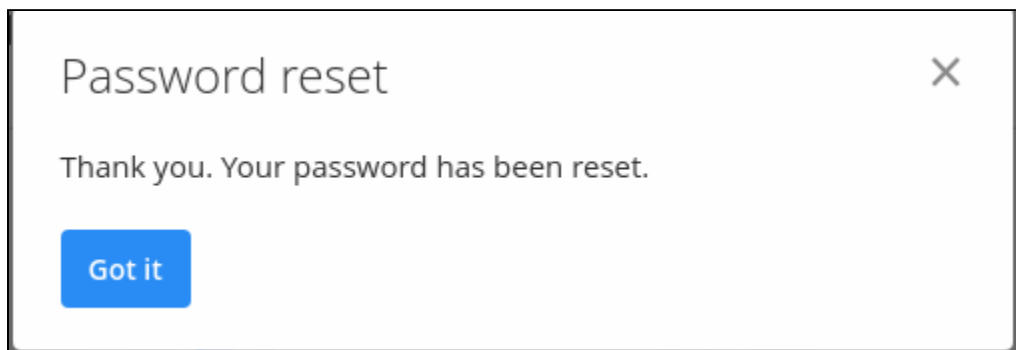


Figure 3: Server Acceptance of the weak password

As a result of the observed restrictions, it was possible for users to set their passwords to simple values such as `tester123`. If a user does use a weak password, it is more likely that an attacker could guess their password and gain access to their account. Alternatively, in the event of a password database breach, an attacker is more likely to recover a weak password from a brute-force attack.

Recommendation

Review the system's documentation and update the password complexity requirements to mandate the use of strong passwords. It is recommended that a minimum password length of 12 characters should be set with three different character classes used. Password reuse should also be disallowed.

Do not require users to regularly update passwords, as this results in weaker passwords overall.⁵

Finally, consider providing users with the option to use multi-factor authentication for all applications.

Location

- <https://s-manage.realvnc.com/en/>

5. NCSC Password policy: updating your approach <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>

Outdated WordPress Plugin

Overall Risk Informational
Impact Undetermined
Exploitability Low

Finding ID NCC-E019128-HET
Component CMS Website
Category Patching
Status New

Description

One WordPress plugin from the CMS web application was outdated and affected by one publicly reported security vulnerability. This indicates there may be a gap within the security patching process.

As shown below, the version in use by the Elementor plugin was 3.25.0, which was affected by CVE-2024-8236⁶. This issue which was exposed by the outdated software could be leveraged by an authenticated attacker (with the Contributor+ role) to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

```
curl https://stage-www.realvnc.com/wp-content/plugins/elementor/assets/js/admin-feedback.js  
↳ 2>&1 | grep -i elementor  
/!* elementor - v3.25.0 - 24-11-2024 */
```

Recommendation

Ensure that the affected plugin is covered by an effective patching policy that allows the latest server software upgrades, updates, or patches to be tested and applied within a short time frame following their release by the vendor. Consideration should be given to enabling the auto-update functionality within the affected third party software, to ensure that updates are applied quickly and regularly.

Location

- <https://stage-www.realvnc.com/wp-content/plugins/elementor/assets/js/admin-feedback.js>
- <https://stage-www.realvnc.com/wp-content/plugins/elementor/assets/css/admin.min.css>

6. Elementor Website Builder < 3.25.8 - Contributor+ Stored XSS: <https://wpscan.com/vulnerability/78f0847b-3f59-43cf-87db-2cadda862aa3/>



Users Can Reuse Old Passwords

Overall Risk Informational

Impact Low

Exploitability Low

Finding ID NCC-E019128-ETJ

Component Real VNC Portal

Category Authentication

Status New

Description

When submitting a new password during a password reset, it is possible for a user to change their password to a previously used password. This goes against best practices for forced password changes. For example:

1. If periodic password changes are required, users can simply change their passwords back to the previously used password. This not only artificially extends the lifetime of user passwords but also increases the likelihood that users will reuse passwords from other, less secure applications.
2. If a user's password is reset in an insecure manner (e.g. the password is emailed to them or read to them by an administrator), then the user can keep the insecure password.

Recommendation

Maintain a previously used password history and a reuse threshold. The history should contain hashes of previously used passwords and not the passwords themselves. Leverage this to prevent users from using a previously set password. Also, limit the number of allowed password changes to one or two per day.

Location

- <https://s-manage.realvnc.com/en/>



Wildcard TLS Certificate in Use

Overall Risk Informational

Impact Low

Exploitability Low

Finding ID NCC-E019128-GYT

Component Real VNC Portal and ODA
Branding Site

Category Cryptography

Status New

Description

The TLS services used wildcard certificates. Such certificates offer a cost-effective means of extending SSL/TLS coverage across multiple servers and applications. However, although wildcard certificates are cryptographically no weaker than dedicated certificates, the effective security level is reduced to that of the weakest application or component. It was therefore notable that the certificate had the potential to be valid for both test and production environments.



The following wildcard certificate were found:

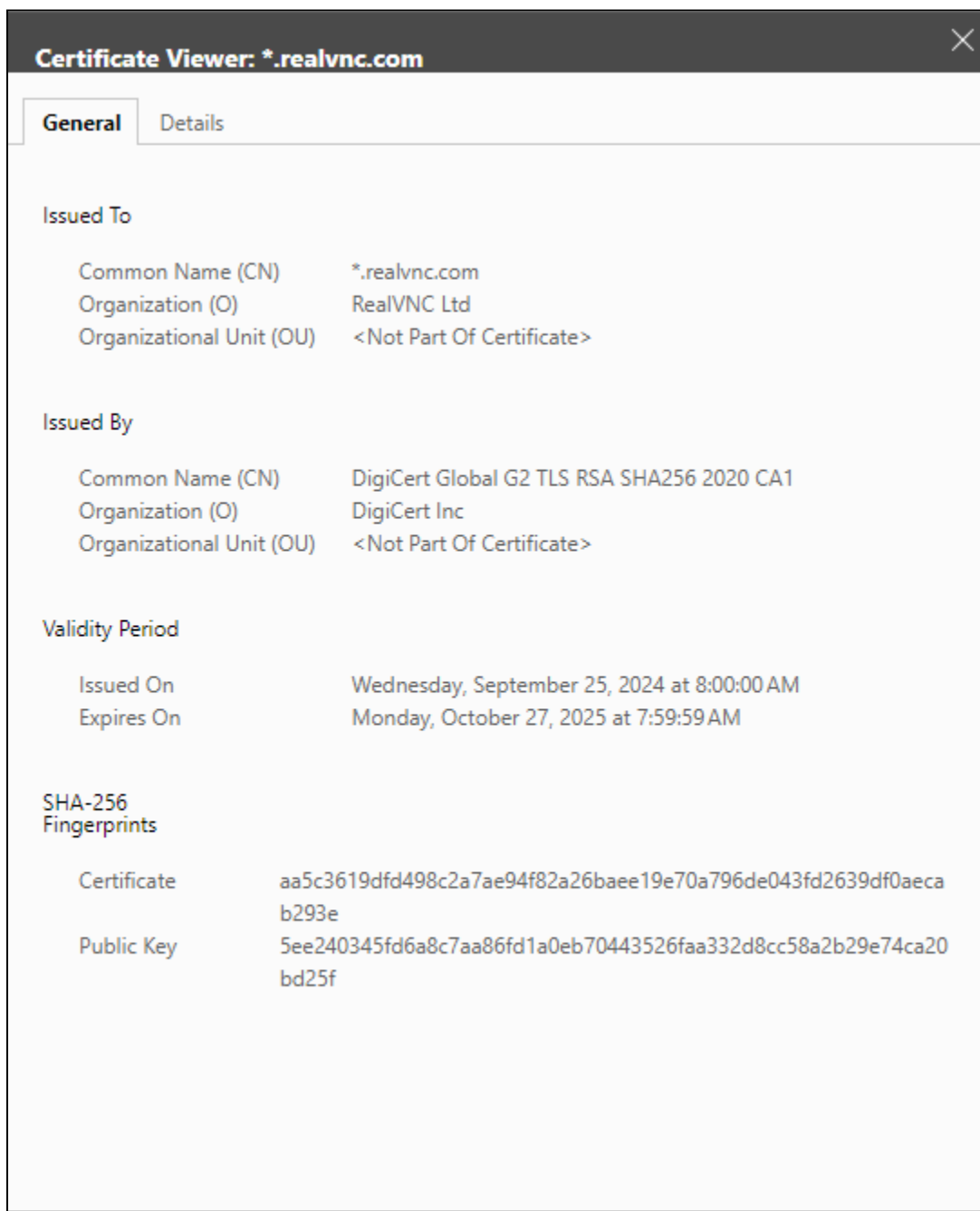


Figure 4: Real VNC Portal Wildcard Certificate

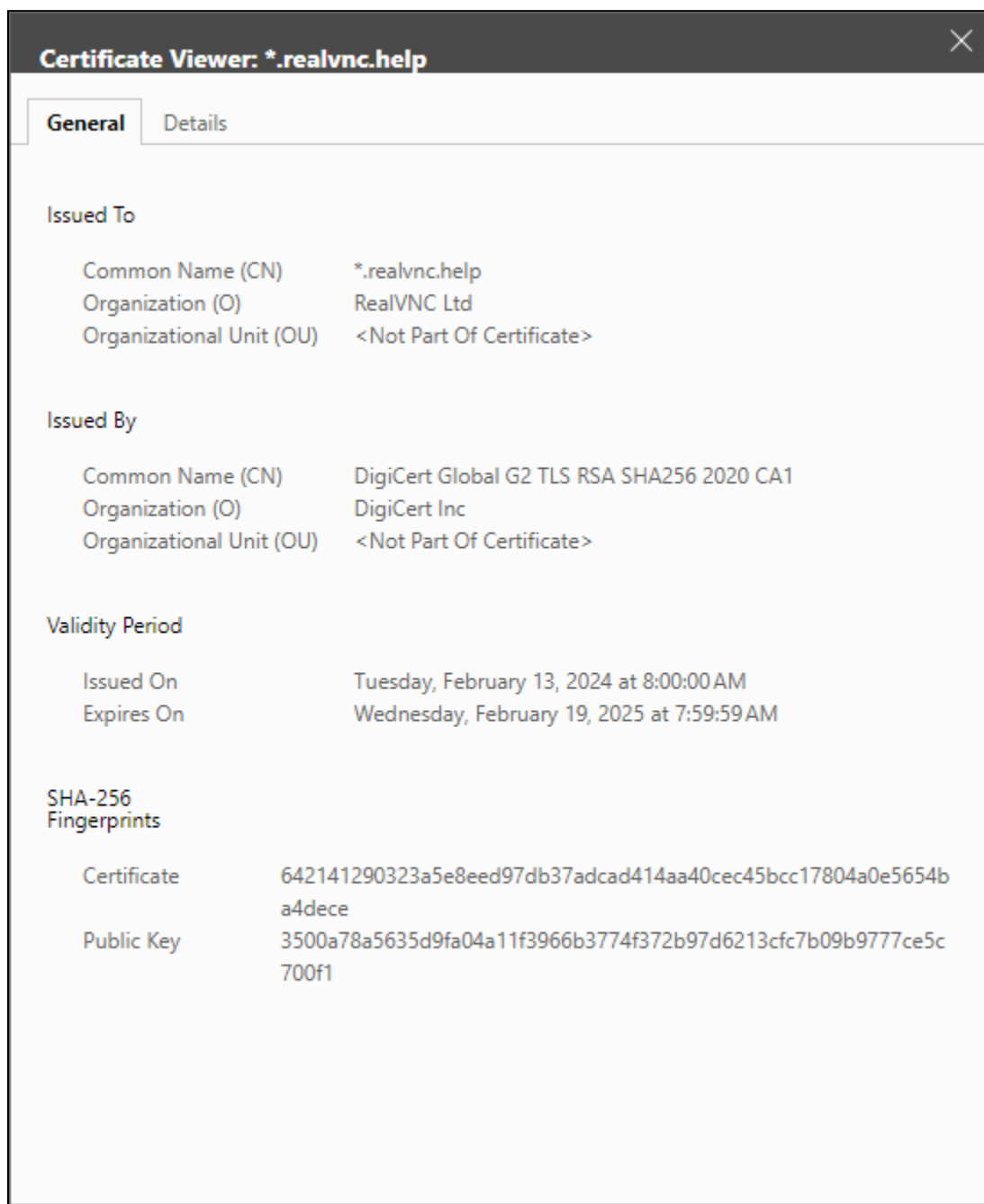


Figure 5: ODA Branding Site Wildcard Certificate

Should an attacker be able to compromise one server or application that uses a wildcard certificate and recover the certificate's private key, it would then be possible to mount a man-in-the-middle attack against any SSL/TLS enabled service in any of the subdomains covered by the wildcard certificate, even if they have a different certificate installed.

Note that Extended Validation Certificates cannot be issued for wildcard certificates.

Recommendation

If possible, make use of a separate certificate for each application or service.

If it is not cost-effective to deploy a separate certificate for each application or service, consider using Subject Alternative Names to allow a certificate to cover multiple hostnames. This would require a new certificate to be issued.

Where certificates are reused, consider the security domains in which they operate. For example, a certificate used for a publicly accessible web forum application of low business importance should not also be used for a business critical web application that processes payments or otherwise handles sensitive information. A similar separation should be considered between test and production environments.^{7 8}

Ensure that incident response processes account for the use of wildcard certificates in the event of a server or application compromise.

Location

- <https://s-manage.realvnc.com/>
- <https://s-www.realvnc.help/>

7. The Risks in Wildcard Certificates: <https://www.sslshopper.com/article-the-risks-in-wildcard-certificates.html>

8. OWASP Transport Layer Protection Cheat Sheet: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet



Username Enumeration

Overall Risk Informational

Impact None

Exploitability Low

Finding ID NCC-E019128-NE6

Component Real VNC Portal

Category Other

Status New

Description

An attacker can more easily identify which usernames are valid for the application, granting them a slight advantage in conducting brute-force attacks. By attempting to log in to the application using a known email address via SSO, NCC Group observed that the application disclosed whether the email address was registered to an existing account. This information can be useful in further attacks, allowing attackers to enumerate a list of valid accounts which can then be used for brute force or phishing attacks. For most applications, it can be difficult or impossible to remediate this attack vector, and preventing users from knowing whether an account is registered can significantly impact the usability of the application. As a result, NCC Group generally recommends that applications evaluate alternative measures for abuse protection rather than attempt to hide whether a given account exists.

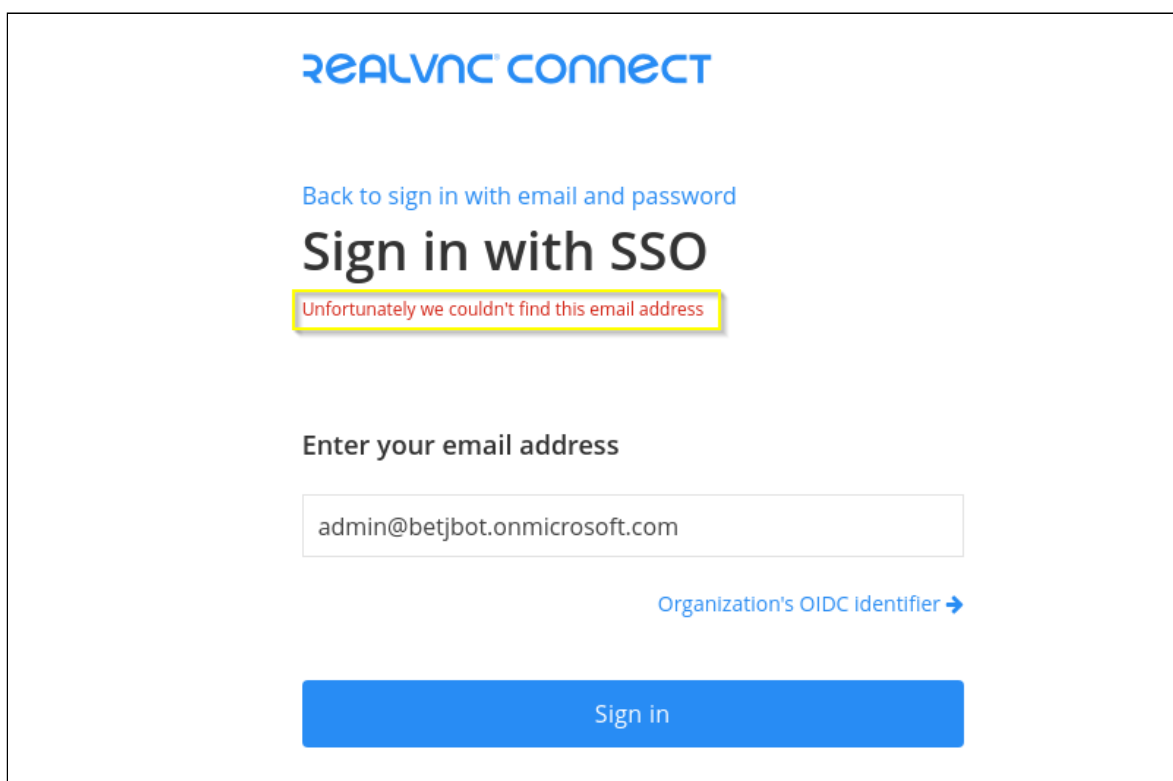
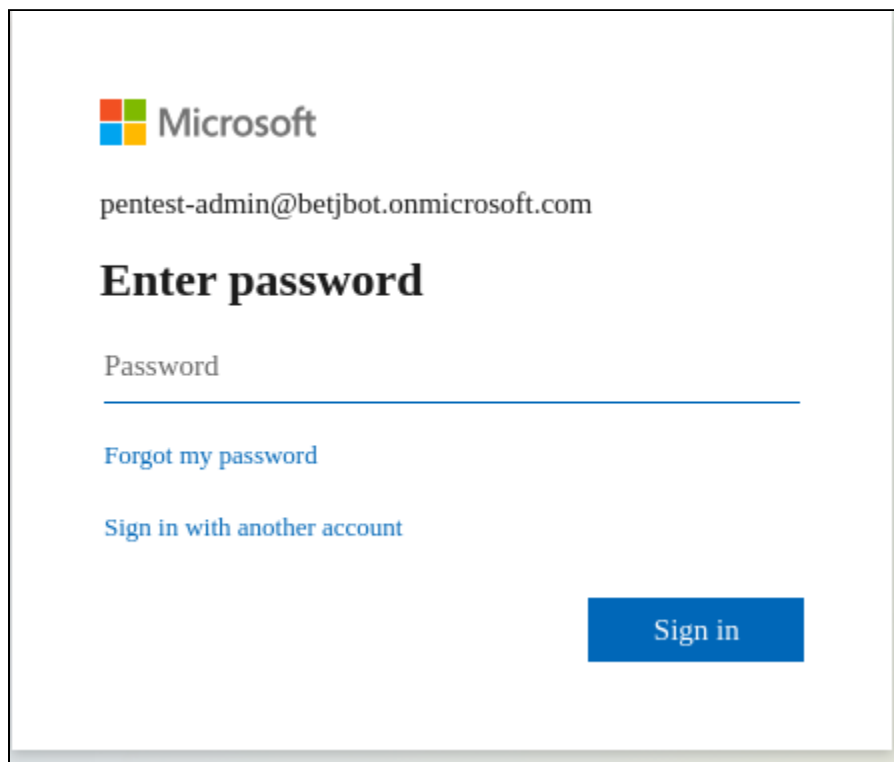


Figure 6: Verbose Error message from a non-existent email address



Microsoft

pentest-admin@betjbot.onmicrosoft.com

Enter password

Password

[Forgot my password](#)

[Sign in with another account](#)

[Sign in](#)

Figure 7: Web app proceeds to the password prompt when email address is valid

Recommendation

Ensure that the system does not differentiate responses based on email validity. Instead of proceeding to a password prompt for valid emails, show the same behaviour and generic response for both valid and invalid email addresses.

Location

- https://s-manage.realvnc.com/en/sso/sign_in

Misconfigured Content Security Policy

Overall Risk Informational
Impact Undetermined
Exploitability Low

Finding ID NCC-E019128-DFC
Component CMS Website
Category Configuration
Status New

Description

The Content Security Policy (CSP)⁹ specified by the application was misconfigured. The CSP header is a powerful mechanism for controlling which external sites can host resources used by an application and how these resources may behave. Using this HTTP header can provide defence in depth from content injection and session-riding attacks, but correct implementation requires a degree of planning to minimise conflicts between policies and actual application behaviour.

The following CSP headers were returned by the application:

```
Content-Security-Policy: frame-ancestors 'self';
```

The `frame-ancestors` directive specifies valid parents that may embed a page using `<frame>`, `<iframe>`, `<object>`, or `<embed>` only. It does not disallow the injection of plugins which can execute JavaScript like an `object-src`

Note that no clear security risk is apparent due to the nature of the application and having protections enforced in the public application, this issue was rated as informational.

Recommendation

Consider defining a list of trusted locations from which JavaScript code can be executed (along with many other restrictions). As the `Content-Security-Policy` header has a large number of options, some of which could conflict with the current implementation, it should be tailored to each specific application after appropriate testing.

An effective CSP generally requires some architectural changes; in particular, JavaScript must be moved to standalone files rather than written inline.^{10 11 12} Move inline JavaScript to standalone files. Then, set a Content Security Policy which allows trusted sources of JavaScript, and disables inline JavaScript.

While developing the policy, a tool such as Google's [CSP Evaluator](#) can be used to check the configuration for security issues.

Location

- <https://stage-www.realvnc.com>

9. Content Security Policy (CSP) - HTTP | MDN: <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

10. An Introduction to Content Security Policy: <https://scotthelme.co.uk/content-security-policy-an-introduction/>

11. MDN Web Docs - Content Security Policy: <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

12. web.dev - Content Security Policy: <https://web.dev/csp/>

