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 2025.1
December 2025

RealVNC® response to the report

The security and privacy of our customers are central to everything we do at RealVNC®. Our flagship product, RealVNC® Connect, is designed from the ground up with robust security and privacy principles at its core. We recognize that our online infrastructure, website, and software must consistently meet the highest security standards and stay ahead of emerging threats.

To ensure continued assurance in our security posture, we engaged NCC Group, an independent security agency, in December 2025 to perform our annual penetration test. Their assessment evaluated our infrastructure and services to deliver an objective, third party report. This document addresses any issues identified in their findings.
The scope of the assessment covered the RealVNC® Connect Portal (including SSO, API access keys, and purchase flows), our CMS website, and the On Demand Assist website.

We consider this an extremely positive outcome, with no critical, high, or medium severity findings identified. The issues reported were limited to Low and Informational categories, many of which we do not consider exploitable or impactful in real world scenarios. In addition, we operate multiple external safeguards to prevent abuse and continuously monitor our services through our 24/7 Security Operations Centre alongside the internal Security team providing protections that are not externally visible but play a vital role in maintaining our security posture.

We are pleased with the positive feedback provided by NCC Group throughout the engagement and in their final report. While this annual penetration test serves as our baseline security assessment, we believe that responsible organisations should go further to demonstrate their commitment to security. For that reason, in addition to our yearly blackbox testing, we also periodically partner with Cure53 to perform comprehensive white box 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 continually monitor and evaluate internal and external factors that could influence our security posture. To learn more about RealVNC® Connect security, you can visit our dedicated security page at https://www.realvnc.com/en/connect/security/. For further information about RealVNC®'s broader Information Security practices, please see 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.

Real VNC Annual Web Application Security Assessment

Real VNC

Version 1.0 – December 15, 2025

Prepared By
James Wilde

Prepared For
Ben May

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 09/12/2025 and 12/12/2025.

The applications under assessment included a product portfolio website and a customer portal for managing their devices, users, and subscriptions.

Overview

The web application assessment was previously carried out in December 2024 as part of the annual security review under proposal O-219331. This year's security assessment confirmed the presence of a number of pre-existing issues, as well as providing new security recommendations. For each phase, a small number of issues were identified and none were assessed to pose more than a low risk. It is recommended that these issues be reviewed and remediated in accordance with a robust defence in depth security strategy, to minimise the risks faced by Real VNC.

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 Web Application Assessment	0	0	0	3	**3**
ODA Branding Web Application Assessment	0	0	0	3	**3**
Portal Web Application Assessment	0	0	0	3	**3**
Total	**0**	**0**	**0**	**9**	**9**

Assessment Summary

Overall, the three in scope websites demonstrated a mature security posture, having benefited from prior testing and the application of several strategic recommendations. They effectively mitigated many common web application vulnerabilities, resulting in a small number of issues being identified.

Common security recommendations for the websites related to TLS/SSL certificate validation, configuration and scope; and DNS infrastructure security (DNSSEC). For example, for certificate validation, both the Portal and ODA websites did not support Online Certificate Status Protocol Stapling (OCSP), which is a more secure mechanism to check whether a TLS/SSL certificate has been revoked. The support for OCSP Stapling addresses privacy concerns of end users by preventing the Certificate Authorities from seeing requests from individual users, as well as improving load times when establishing a secure connection (HTTPS). It was noted that OCSP Stapling was supported by the CMS website.

The in scope websites were configured with a Content Security Policy (CSP), which is a mechanism for regulating which external sites can host resources used by an application, and how these resources may behave. Minor refinements to the CSP are recommended to strengthen the websites' resilience against web application threats. Although no cross-site scripting (XSS) vulnerabilities were identified, a securely configured CSP header configuration will provide a secondary layer of defence.

The Portal application demonstrated a robust security framework, which addressed multiple common web security risks. For example, malicious user input was handled securely, and robust access controls prevented users from accessing privileged areas of the application or data beyond their team or organisation. The application implemented several account takeover controls, including rate limiting and temporarily blocking brute-force attempts

based on originating IP addresses. It also supported multi-factor authentication (MFA) (although this was not mandatory for users) to mitigate credential-based attacks, and required user validation for login attempts from new IP locations.

The assessment highlighted a handful of findings which represented minor variances from standard security best practice. For example, additional defensive measures could be implemented, since the application lacked alerts for repeated failed login attempts and did not enforce temporary account lockouts. One potential attack path involves a slow-paced password guessing attempt designed to remain below the rate-limit threshold. If the attacker's IP address was blocked, the attack could be resumed by changing the originating IP, for example through a VPN. The risk of password compromise was further increased by the server not fully enforcing the client-side password complexity requirements.

The WordPress Content Management System (CMS) website used a small number of plugins that extended the functionality of the site. Several of these plugins were outdated and potentially susceptible to publicly disclosed vulnerabilities affecting their versions. However, it appeared that no technical details were publicly available about these vulnerabilities at the time of writing, which meant it was not possible to confirm whether the website was affected by the outdated plugins.

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 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

Although no significant risks were identified in this assessment, it is recommended that the issues identified in this report be addressed through a structured remediation program, with actions prioritised according to the organisation's risk exposure.

A portion of the findings were attributable from hosts that were not configured with optimal security settings. 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.

It is acknowledged that some of the issues set out in this report were identified because of the nature of the environment (staging) in which the assessment was performed. Nevertheless, they are reported here so that it may be ensured that these issues are not present when these systems are migrated to a production environment.

2 Table of Contents

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	E029530
Proposal Reference	O-233433
Document Title	Real VNC Annual Web Application Security Assessment
Author	James Wilde

Document History

Version	Issue Date	Issued by	Change Description
0.1	2025-12-12	James Wilde	Draft for NCC Group internal review only
0.2	2025-12-15	Harry Aylott	Revised QA
1.0	2025-12-15	James Wilde	Released to client

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 targeted components listed below:

Web Application Assessment

- Portal:
  - https://s-manage.realvnc.com
  - https://s-connect-api.services.vnc.com
- CMS website:
  - https://stage-www.realvnc.com
- ODA branding site:
  - https://s-www.realvnc.help

The Portal's scope covered four user roles: Admin, Manager, User and Technician. The scope of the CMS (WordPress) website encompassed its publicly accessible pages, which did not require user accounts.

Caveats

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.

CMS Web Application Assessment

Title	Status	ID	Risk
DNS Security Extension (DNSSEC) Not in Use	New	JN2	Low
Misconfigured Content Security Policy	New	BLH	Low
Outdated WordPress Plugins	New	JJL	Low
Weak TLS Ciphers	New	7CP	Info

ODA Branding Web Application Assessment

Title	Status	ID	Risk
No Online Certificate Status Protocol (OCSP) Stapling	New	EDQ	Low
Misconfigured Content Security Policy	New	9LY	Low
DNS Security Extension (DNSSEC) Not in Use	New	VQJ	Low
Wildcard SSL Certificate in Use	New	V7P	Info
Weak TLS Cipher Suite Configuration	New	HEJ	Info
Third-Party Script Included Without Subresource Integrity Hash	New	UN2	Info

Portal Web Application Assessment

Title	Status	ID	Risk
Content Security Policy Recommendations	New	BUQ	Low
DNS Security Extension (DNSSEC) Not in Use	New	RP3	Low
No Online Certificate Status Protocol (OCSP) Stapling	New	HKX	Low
Password Policy and Implementation Recommendations	New	CLW	Info
Weak TLS Cipher Suite Configuration	New	UYE	Info
Third-Party Script Included Without Subresource Integrity Hash	New	3UM	Info
Account Takeover (ATO) Protection Recommendations	New	TDJ	Info
Wildcard SSL Certificate in Use	New	6AJ	Info
Password Reset Token Recommendations	New	YFE	Info
Session Invalidation Observation	New	AAU	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 – CMS Web Application Assessment

Low

DNS Security Extension (DNSSEC) Not in Use

Overall Risk	Low	**Finding ID**	NCC-E029530-JN2
Impact	Medium	**Component**	CMS Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

The realvnc site domain did not use 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.

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

Evidence is shown below:

```
$ dnsrecon -d stage-www.realvnc.com -s

[*] std: Performing General Enumeration against: stage-www.realvnc.com...
[-] DNSSEC is not configured for stage-www.realvnc.com
[*]      SOA ns1.cloudflare.net 172.64.40.250
[*]      SOA ns1.cloudflare.net 108.162.198.250
[*]      SOA ns1.cloudflare.net 162.159.60.250
[*]      SOA ns1.cloudflare.net 2606:4700:57:1:4e4b:27d7:a29f:3cfa
[*]      SOA ns1.cloudflare.net 2803:f800:52:1:1df9:cfa1:ac40:28fa
[*]      SOA ns1.cloudflare.net 2a06:98c1:56:1:2693:f8af:6ca2:c6fa
[*]      CNAME stage-www.realvnc.com stage-www.realvnc.com.cdn.cloudflare.net
[*]      A stage-www.realvnc.com.cdn.cloudflare.net 172.67.204.74
[*]      A stage-www.realvnc.com.cdn.cloudflare.net 104.21.58.134
[*]      CNAME stage-www.realvnc.com stage-www.realvnc.com.cdn.cloudflare.net
[*]      AAAA stage-www.realvnc.com.cdn.cloudflare.net 2606:4700:3034::ac43:cc4a
[*]      AAAA stage-www.realvnc.com.cdn.cloudflare.net 2606:4700:3035::6815:3a86
[*] Enumerating SRV Records
[-] No SRV Records Found for stage-www.realvnc.com
```

Recommendation

It is recommended that DNSSEC should be implemented on the realvnc site domain. Consult with your registrar on how this can be performed.[1][2]

Reproduction Steps

Retrieve the DNSSEC status from domain WHOIS records using the `whois` utility, or query a third-party service such as DNSSEC Analyzer.

Location

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

1. DNSSEC: https://technet.microsoft.com/en-us/library/jj200221.aspx, https://www.dnssec.net/
2. DNSSEC Analyzer: https://dnssec-debugger.verisignlabs.com/

Low

Misconfigured Content Security Policy

Overall Risk	Low	**Finding ID**	NCC-E029530-BLH
Impact	Medium	**Component**	CMS Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

The Content Security Policy (CSP)[3] 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 realvnc site CSP included a single directive, `frame-ancestors`, which focused on Clickjacking [4] protection by restricting framing to the same origin, thus blocking external sites from embedding the application. However, the CSP could be modified by including the `default-src` fallback directive [5], in order to provide additional protective measures against XSS.

Recommendation

Consider updating the CSP by including the `default-src` 'self' as fallback:

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

An effective CSP generally requires some architectural changes; in particular, JavaScript must be moved to standalone files rather than written inline.[6] [7] [8] 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[9] can be used to check the configuration for security issues.

Location

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

3. Content Security Policy (CSP) - HTTP | MDN: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
4. OWASP - Clickjacking: https://owasp.org/www-community/attacks/Clickjacking
5. The default-src Directive: https://content-security-policy.com/default-src/
6. An Introduction to Content Security Policy: https://scotthelme.co.uk/content-security-policy-an-introduction/
7. MDN Web Docs - Content Security Policy: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
8. web.dev - Content Security Policy: https://web.dev/csp/
9. CSP Evaluator: https://csp-evaluator.withgoogle.com

Low

Outdated WordPress Plugins

Overall Risk	Low	**Finding ID**	NCC-E029530-JJL
Impact	Medium	**Component**	CMS Web Application Assessment
Exploitability	Undetermined	**Category**	Patching
		Status	New

Description

Several plugins installed on the WordPress CMS were outdated and exposed to publicly reported vulnerabilities that may be exploitable in certain circumstances.

The following outdated WordPress plugins were identified:

- Elementor and Elementor-pro
  - Version: 3.32.5 (Elementor) and 3.32.3 (Elementor-pro)
  - Vulnerability: CVE-2025-67588 - missing authorisation flaw in Elementor Website Builder that may allow attackers to gain unauthorised access to sensitive functionalities.
  - Latest stable version: 3.33.4 (Elementor), 3.33.2 (Elementor-pro)
- HubSpot WordPress Plugin
  - Version: 11.3.16
  - Vulnerability: CVE-2025-11762 - sensitive plugin data exposure to low-privilege users.
  - Latest stable version: 11.3.33

It should be noted that while both CVEs are disclosed and catalogued, exploit code and technical specifics have not yet been made available in recognised PoC repositories or official advisories.

Recommendation

Update the outdated WordPress plugins to the latest stable and non-vulnerable version.

Consideration should be given to enabling the auto-update for plugins where possible,[10] [11] to ensure that updates are applied quickly and regularly.

Location

- https://stage-www.realvnc.com/wp-content/plugins/elementor/changelog.txt
- https://stage-www.realvnc.com/wp-content/plugins/elementor-pro/changelog.txt
- https://stage-www.realvnc.com/wp-content/plugins/leadin/changelog.txt

10. Outdated Plugin Notifier: https://wordpress.org/plugins/outdated-plugin-notifier/
11. Vendi Abandoned Plugin Check: https://wordpress.org/plugins/vendi-abandoned-plugin-check/

Info

Weak TLS Ciphers

Overall Risk	Informational	**Finding ID**	NCC-E029530-7CP
Impact	Low	**Component**	CMS Web Application Assessment
Exploitability	Medium	**Category**	Configuration
		Status	New

Description

Some cipher suites supported by two of the hosts in scope were not sufficiently cryptographically secure and, as a result, cannot provide as much protection against brute-force decryption when compared to more modern cipher suites, should the traffic be captured.

The following cipher suites were supported, with the weak ciphers[12] highlighted in yellow. Note that the weak ciphers were *not* the preferred option.

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
```

Recommendation

Consult the server's documentation to disable weak cipher suites. Follow Mozilla's recommendation[13] for more guidance on general configuration of TLS. Mozilla's SSL Configuration Generator[14] provides a straightforward way to generate secure configuration for many common servers.

Reproduction Steps

Use a tool such as SSLyze (available at https://github.com/nabla-c0d3/sslyze) or testssl.sh to identify the protocols, cipher suites, and cryptographic parameters supported by the listed servers.

12. TLS Ciphersuite Search: https://ciphersuite.info/
13. Mozilla - Server Side TLS: https://wiki.mozilla.org/Security/Server_Side_TLS
14. Mozilla - SSL Configuration Generator: https://ssl-config.mozilla.org/

Location

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

8 Finding Details – ODA Branding Web Application Assessment

Low

No Online Certificate Status Protocol (OCSP) Stapling

Overall Risk	Low	**Finding ID**	NCC-E029530-EDQ
Impact	Low	**Component**	ODA Branding Web Application Assessment
Exploitability	Low	**Category**	Cryptography
		Status	New

Description

The TLS certificates offered by the ODA branding site did not offer OCSP stapling, a technology that builds upon certificate revocation technology and is used to provide a more reliable and secure method for a client to determine the revocation status of any particular TLS certificate.

With traditional certificate revocation methods, it is up to the client to retrieve Certificate Revocation Lists (CRLs). As this is a resource intensive process this can result in a failure to retrieve the required information and also can negatively affect the user experience.

Evidence is provided below:

```
$ ./testssl.sh s-www.realvnc.help
{REMOVED FOR BREVITY}

 OCSP URI                     http://ocsp.digicert.com
 OCSP stapling                not offered
 OCSP must staple extension   --
```

Standard OCSP performs similar checks to traditional certificate revocation list (CRL) methods, but is considered more reliable and does not require large lists of information to be retrieved. However, the client is still required to communicate with the CA directly, which can lead to issues similar to those found with traditional CRL methods.

OCSP stapling removes the responsibility from the client to verify with the CA directly. Instead, the server regularly polls the CA and obtains time stamped signed data. This is then stapled onto the TLS response to the client so that the client can verify if the connection is legitimate. This reduces the resource overhead of the technique and so reduces much of the negative consequences associated with traditional CRLs and regular OCSP.[15] [16]

Recommendation

Although OCSP stapling has a number of benefits, as a technology it is not widely adopted and browser support varies. It is recommended that the technology is reviewed to determine if it can be deployed to the existing platform.

Location

- https://s-www.realvnc.help

15. Everything You Need to Know About OCSP, OCSP Stapling and OCSP Must-Staple - https://www.thesslstore.com/blog/ocsp-ocsp-stapling-ocsp-must-staple/
16. RFC 6960 - Online Certificate Status Protocol – OCSP https://tools.ietf.org/html/rfc6960

Low

Misconfigured Content Security Policy

Overall Risk	Low	**Finding ID**	NCC-E029530-9LY
Impact	Medium	**Component**	ODA Branding Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

The ODA branding site specified a Content Security Policy (CSP)[17], albeit in report only mode. 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 header was returned by the application:

```
Content-Security-Policy-Report-Only: connect-src *.analytics.google.com *.google-
↳ analytics.google.com stats.g.doubleclick.net www.facebook.com ws.zoominfo.com; default-src
↳ 'self' 'unsafe-eval' 'unsafe-inline' blob: dev.visualwebsiteoptimizer.com fonts.gstatic.com
↳ forms.hubspot.com js-na1.hs-scripts.com js.hs-analytics.net js.hs-banner.com
↳ js.hsleadflows.net r1.visualwebsiteoptimizer.com r2.visualwebsiteoptimizer.com
↳ r3.visualwebsiteoptimizer.com track.hubspot.com www.google-analytics.com
↳ www.googletagmanager.com s-static.realvnc.com s-static.realvnc.help; img-src
↳ www.facebook.com t.co analytics.twitter.com px.ads.linkedin.com s-www.realvnc.help; script-
↳ src static.ads-twitter.com snap.licdn.com connect.facebook.net; script-src-elem static.ads-
↳ twitter.com snap.licdn.com connect.facebook.net code.jquery.com static.ads-twitter.com
↳ snap.licdn.com static.hotjar.com script.hotjar.com tracking.g2crowd.com sc.lfeeder.com www.go
↳ ogle.com www.gstatic.com waw.chat.getzowie.com realvnc.chat.getzowie.com dev.zopim.com
↳ www.google-analytics.com www.google.com www.googletagmanager.com www.gstatic.com js-na1.hs-
↳ scripts.com js.hs-analytics.net js.hs-banner.com js.hsleadflows.net s-www.realvnc.help;
↳ report-uri https://a2e4a722b4dffeb32eefdbbef3440333.report-uri.com/r/d/csp/reportOnly;
```

A large number of third-party domains were allowlisted within the policy. Every allowlisted domain undermines the CSP and potentially allows for exploitation of XSS vulnerabilities which would otherwise not be exploitable. In particular, several allowlisted domains (highlighted above) were known to allow various CSP bypasses.[18] [19] [20]

The policy also declared 'unsafe-eval' 'unsafe-inline' in the `default-src`[21] fallback policy. However, because of the CSP's precedence rules,[22] the `default-src` configuration no longer applied to JavaScript execution, as any 'unsafe-inline' or 'unsafe-eval' in `default-src` will be ignored for scripts because the CSP defined `script-src` and `script-src-elem` directives.

17. Content Security Policy (CSP) - HTTP | MDN: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
18. Content Security Bypass Techniques to perform XSS - Medium: https://medium.com/@bhaveshthakur2015/content-security-policy-csp-bypass-techniques-e3fa475bfe5d
19. Content Security Policy Bypass - Deteact - continuous information security services: https://blog.deteact.com/csp-bypass/
20. Content Security Policy (CSP) Bypass - HackTricks: https://book.hacktricks.xyz/pentesting-web/content-security-policy-csp-bypass
21. The default-src Directive: https://content-security-policy.com/default-src/
22. CSP3 - Fetch Directives: https://www.w3.org/TR/CSP3/#fetch-directives

Note that if both `script-src` and `script-src-elem` directives were removed, then the declaration of 'unsafe-eval' 'unsafe-inline' for `default-src` would enable XSS attacks by allowing code to be included directly into the document.

The CSP was also in `Report-Only` mode, meaning any CSP violations would not take effect. [23] The policy should be switched to enforcing mode as soon as it has been tested and the efficacy of the proposed policy confirmed.

Recommendation

Review the CSP's configuration to implement security best practice as described by the specification.[24] [25] [26] [27] [28]

Review the allowlisted third-party domains and only allow domains that are strictly necessary. Furthermore, both `script-src` and `script-src-elem` have overlapping domains, with `script-src-elem` overriding `script-src` for external scripts. Consider consolidating into `script-src` only, unless there is a requirement to use the more granular controls of `script-src-elem`.

While developing the policy, a tool such as Google's CSP Evaluator[29] can be used to check the configuration for security issues.

Location

- https://s-www.realvnc.help

23. MDN - Content-Security-Policy-Report-Only Header: https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Content-Security-Policy-Report-Only
24. Content Security Policy Level 3: https://www.w3.org/TR/CSP3/
25. Content Security Policy Reference: https://content-security-policy.com/
26. An Introduction to Content Security Policy: https://scotthelme.co.uk/content-security-policy-an-introduction/
27. MDN Web Docs - Content Security Policy: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
28. web.dev - Content Security Policy: https://web.dev/csp/
29. CSP Evaluator: https://csp-evaluator.withgoogle.com

Low

DNS Security Extension (DNSSEC) Not in Use

Overall Risk	Low	**Finding ID**	NCC-E029530-VQJ
Impact	Medium	**Component**	ODA Branding Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

The ODA branding site domain did not use 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.

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

```
$ dnsrecon -d s-www.realvnc.help
2025-12-11T10:16:30.131187+0000 INFO Starting enumeration for domain: s-www.realvnc.help
2025-12-11T10:16:30.131721+0000 INFO std: Performing General Enumeration against: s-
↳www.realvnc.help...
2025-12-11T10:16:30.369543+0000 ERROR No answer for DNSSEC query for s-www.realvnc.help
2025-12-11T10:16:30.635266+0000 INFO     A s-www.realvnc.help 146.101.15.122
2025-12-11T10:16:30.795452+0000 INFO Enumerating SRV Records
2025-12-11T10:16:33.939345+0000 ERROR No SRV Records Found for s-www.realvnc.help
2025-12-11T10:16:33.939936+0000 INFO Completed enumeration for domain: s-www.realvnc.help
```

Recommendation

It is recommended that DNSSEC should be implemented on the ODA branding site domain. Consult with your registrar on how this can be performed.[30]

Reproduction Steps

https://s-www.realvnc.help

Location

- https://s-www.realvnc.help

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

Info

Wildcard SSL Certificate in Use

Overall Risk	Informational	**Finding ID**	NCC-E029530-V7P
Impact	Low	**Component**	ODA Branding Web Application Assessment
Exploitability	Low	**Category**	Cryptography
		Status	New

Description

The ODA branding site used a wildcard SSL certificate. 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 certificates was found:

```
$ sslscan s-www.realvnc.help
{REMOVED FOR BREVITY}

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.realvnc.help
Altnames: DNS:*.realvnc.help, DNS:realvnc.help
Issuer:   DigiCert Global G2 TLS RSA SHA256 2020 CA1
```

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.

If the wildcard certificate is used on any service that allows SSLv2 connections, then this service may be vulnerable to the DROWN attack.

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.[31] [32]

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

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

Location

- https://s-www.realvnc.help

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

Info

Weak TLS Cipher Suite Configuration

Overall Risk	Informational	**Finding ID**	NCC-E029530-HEJ
Impact	Low	**Component**	ODA Branding Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

Some cipher suites supported by two of the hosts in scope were not sufficiently cryptographically secure and, as a result, cannot provide as much protection against brute-force decryption when compared to more modern cipher suites, should the traffic be captured.

The following cipher suites were supported, with the weak ciphers[33] highlighted in yellow. Note that the weak ciphers were *not* the preferred option.

```
TLSv1.2 (server order)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLSv1.3 (server order)
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
```

Recommendation

Consult the server's documentation to disable weak cipher suites. Follow Mozilla's recommendation[34] for more guidance on general configuration of TLS. Mozilla's SSL Configuration Generator[35] provides a straightforward way to generate secure configuration for many common servers.

Location

- https://s-www.realvnc.help

33. TLS Ciphersuite Search: https://ciphersuite.info/
34. Mozilla - Server Side TLS: https://wiki.mozilla.org/Security/Server_Side_TLS
35. Mozilla - SSL Configuration Generator: https://ssl-config.mozilla.org/

Info

Third-Party Script Included Without Subresource Integrity Hash

Overall Risk	Informational	**Finding ID**	NCC-E029530-UN2
Impact	Low	**Component**	ODA Branding Web Application Assessment
Exploitability	Low	**Category**	Other
		Status	New

Description

The ODA branding site used JavaScript hosted by a third party. This creates the risk that a compromise of the third party script host could result in a compromise of the application's users. Specifically, if an attacker compromises the third party host, they could replace the script with a malicious script that completely controls user accounts. Third party JavaScript has been documented as a source of site compromise in the past.[36]

In order to mitigate this risk, Subresource Integrity (SRI)[37] was introduced as a browser feature in most major browsers.[38] This feature allows web applications to specify a hash of a script included with a `<script>` tag in order to verify the file has not been modified. Unfortunately, this feature has only received limited support from the vendors who most commonly provide hosted JavaScript. If the vendor does not support SRI, then the only choices may be to keep the functionality as is, or to remove the script and associated functionality.

The following external script was referenced:

- https://code.jquery.com/jquery-3.6.0.min.js

Recommendation

Ideally, active content such as JavaScript, CSS, HTML, Java or Flash code should be hosted locally, rather than be included from third party hosts. If external hosting is preferred – usually for the performance gains delivered by content delivery networks (CDNs) – it is recommended that only reputable third parties are used and that, in the case of script and CSS files, the SRI attribute is added to force an integrity check. SRI specifies an encoded hash of the expected file, which conforming browsers will verify; for example:

```
<script src="//some.other.site.com/jquery/jquery.min.js" integrity="sha384-I6F5OKECLVtK/
↳BL+8iSLDEHowSAfUo76ZL9+kGAgTRdiByINKJaqTPH/QVNS1VDb" crossorigin="anonymous"></script>
```

In this case, should the hash of the file received by the browser from the third party not match the value specified by the first party, the script will not be loaded. For more information on SRI implementation and browser support, see the footnotes, but note that SRI:

- Will prove problematic with resources that change without notice (and therefore it may be preferable to reference a specific version rather than the 'latest' version)

36. The JavaScript Supply Chain Paradox: SRI, CSP and Trust in Third Party Libraries: https://www.troyhunt.com/the-javascript-supply-chain-paradox-sri-csp-and-trust-in-third-party-libraries/
37. Mozilla - Subresource Integrity (SRI): https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
38. Can I use - Subresource Integrity: https://caniuse.com/#feat=subresource-integrity

- Requires the `crossorigin` attribute
- Cannot check the integrity of scripts that are loaded dynamically
- Provides no effective protection if the first party page is delivered over HTTP

Location

- https://s-www.realvnc.help

9 Finding Details – Portal Web Application Assessment

Low

Content Security Policy Recommendations

Overall Risk	Low	**Finding ID**	NCC-E029530-BUQ
Impact	Medium	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

The Content Security Policy (CSP)[39] specified by the Portal web application had scope for enhancement. 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 header was returned by the application:

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

The Portal's CSP included a single directive, `frame-ancestors`, which focused on Clickjacking[40] protection by restricting framing to the same origin, thus blocking external sites from embedding the application. However, the CSP could be improved by including the `default-src` fallback directive[41], so as to provide additional protective measures against XSS.

Recommendation

Consider updating the CSP by including the `default-src` 'self' as fallback:

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

An effective CSP generally requires some architectural changes; in particular, JavaScript must be moved to standalone files rather than written inline.[42] [43] [44] 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[45] can be used to check the configuration for security issues.

Location

- https://s-manage.realvnc.com

39. Content Security Policy (CSP) - HTTP | MDN: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
40. OWASP - Clickjacking: https://owasp.org/www-community/attacks/Clickjacking
41. The default-src Directive: https://content-security-policy.com/default-src/
42. An Introduction to Content Security Policy: https://scotthelme.co.uk/content-security-policy-an-introduction/
43. MDN Web Docs - Content Security Policy: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
44. web.dev - Content Security Policy: https://web.dev/csp/
45. CSP Evaluator: https://csp-evaluator.withgoogle.com

Low

DNS Security Extension (DNSSEC) Not in Use

Overall Risk	Low	**Finding ID**	NCC-E029530-RP3
Impact	Medium	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

The Portal domain did not use 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.

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.

Evidence is shown below:

```
$ dnsrecon -d s-manage.realvnc.com
2025-12-11T09:57:05.212106+0000 INFO Starting enumeration for domain: s-manage.realvnc.com
2025-12-11T09:57:05.212740+0000 INFO std: Performing General Enumeration against: s-
↳manage.realvnc.com...
2025-12-11T09:57:05.288154+0000 ERROR No answer for DNSSEC query for s-manage.realvnc.com
2025-12-11T09:57:05.413124+0000 INFO     SOA ns1.cloudflare.net 172.64.40.250
2025-12-11T09:57:05.413294+0000 INFO     SOA ns1.cloudflare.net 162.159.60.250
2025-12-11T09:57:05.413383+0000 INFO     SOA ns1.cloudflare.net 108.162.198.250
2025-12-11T09:57:05.413478+0000 INFO     SOA ns1.cloudflare.net 2a06:98c1:56:1:2693:f8af:
↳6ca2:c6fa
2025-12-11T09:57:05.413575+0000 INFO     SOA ns1.cloudflare.net
↳2803:f800:52:1:1df9:cfa1:ac40:28fa
2025-12-11T09:57:05.413672+0000 INFO     SOA ns1.cloudflare.net 2606:4700:57:1:4e4b:27d7:a29f:
↳3cfa
2025-12-11T09:57:05.558869+0000 INFO     CNAME s-manage.realvnc.com s-
↳manage.realvnc.com.cdn.cloudflare.net
2025-12-11T09:57:05.559260+0000 INFO     A s-manage.realvnc.com.cdn.cloudflare.net
↳172.67.204.74
2025-12-11T09:57:05.559493+0000 INFO     A s-manage.realvnc.com.cdn.cloudflare.net
↳104.21.58.134
2025-12-11T09:57:05.559818+0000 INFO     CNAME s-manage.realvnc.com s-
↳manage.realvnc.com.cdn.cloudflare.net
2025-12-11T09:57:05.560177+0000 INFO     AAAA s-manage.realvnc.com.cdn.cloudflare.net
↳2606:4700:3035::6815:3a86
2025-12-11T09:57:05.560343+0000 INFO     AAAA s-manage.realvnc.com.cdn.cloudflare.net
↳2606:4700:3034::ac43:cc4a
2025-12-11T09:57:05.801040+0000 INFO Enumerating SRV Records
2025-12-11T09:57:06.334272+0000 ERROR No SRV Records Found for s-manage.realvnc.com
2025-12-11T09:57:06.334525+0000 INFO Completed enumeration for domain: s-manage.realvnc.com
```

Recommendation

It is recommended that DNSSEC should be implemented on the Portal domain. Consult with your registrar on how this can be performed.[46]

Location

- https://s-manage.realvnc.com

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

Low

No Online Certificate Status Protocol (OCSP) Stapling

Overall Risk	Low	**Finding ID**	NCC-E029530-HKX
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Cryptography
		Status	New

Description

The TLS certificates offered by the Portal's API host did not offer OCSP stapling, a technology that builds upon certificate revocation technology and is used to provide a more reliable and secure method for a client to determine the revocation status of any particular TLS certificate.

With traditional certificate revocation methods, it is up to the client to retrieve Certificate Revocation Lists (CRLs). As this is a resource intensive process this can result in a failure to retrieve the required information and also can negatively affect the user experience.

Evidence is provided below:

```
$ ./testssl.sh s-connect-api.services.vnc.com
{REMOVED FOR BREVITY}

 OCSP URI                     http://ocsp.digicert.com
OCSP stapling                 not offered
OCSP must staple extension    --
```

Standard OCSP performs similar checks to traditional certificate revocation list (CRL) methods, but is considered more reliable and does not require large lists of information to be retrieved. However, the client is still required to communicate with the CA directly, which can lead to issues similar to those found with traditional CRL methods.

OCSP stapling removes the responsibility from the client to verify with the CA directly. Instead, the server regularly polls the CA and obtains time stamped signed data. This is then stapled onto the TLS response to the client so that the client can verify if the connection is legitimate. This reduces the resource overhead of the technique and so reduces much of the negative consequences associated with traditional CRLs and regular OCSP.[47] [48]

Recommendation

Although OCSP stapling has a number of benefits, as a technology it is not widely adopted and browser support varies. It is recommended that the technology is reviewed to determine if it can be deployed to the existing platform.

Location

- https://s-connect-api.services.vnc.com

47. Everything You Need to Know About OCSP, OCSP Stapling and OCSP Must-Staple - https://www.thesslstore.com/blog/ocsp-ocsp-stapling-ocsp-must-staple/
48. RFC 6960 - Online Certificate Status Protocol – OCSP https://tools.ietf.org/html/rfc6960

Info

Password Policy and Implementation Recommendations

Overall Risk	Informational	**Finding ID**	NCC-E029530-CLW
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Authentication
		Status	New

Description

Although the RealVNC Portal implemented a password complexity estimator, the password restrictions were not enforced server-side. As a result, users could set weak passwords that may be easy to guess by an attacker. Furthermore, a password reuse discrepancy was identified between the Change Password and Forgotten Password mechanisms.

It was noted, however, that the Portal implemented other defences that could assist in limiting or preventing unauthorised access to the application, in the event that a user's password was guessed or compromised. For example, the application blocked login attempts if the user originated from a new IP address. The user would receive an email alerting them to the potentially malicious activity, and a hyperlink that included a short-lived authorisation token to approve the login. Furthermore, the application also provided two-step verification for all user roles, which provided a further layered defence if a user's credentials were compromised.

No Server-Side Enforcement of Password Policy

The RealVNC Portal implemented a password complexity estimator, which encouraged users in choosing strong passwords by providing feedback to the user on password quality whilst they set a password. However, the password strength recommendations appeared not be enforced server-side, meaning that users could choose to ignore the advice and proceed with setting a weak password. Weak passwords can be easier to guess or to determine through a brute-force attack and could therefore increase the risk of account compromise.

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

Password Complexity Recommendations

The password policy enforced by the Portal was insufficient with respect to its minimum length requirement, which was 8 characters. Longer passwords provide a greater combination of characters and consequently make it more difficult for an attacker to guess. Furthermore, there appeared to be no requirement for inclusion of at least one upper and one lower case letter, one digit and one special character.

Password Reuse Discrepancy

A discrepancy in the reuse of passwords was identified between the Change Password and Password Reset functionality. The Change Password functionality (accessible from Profile > Security) prevented users from setting a new password to be the same value as their original password, as shown below:

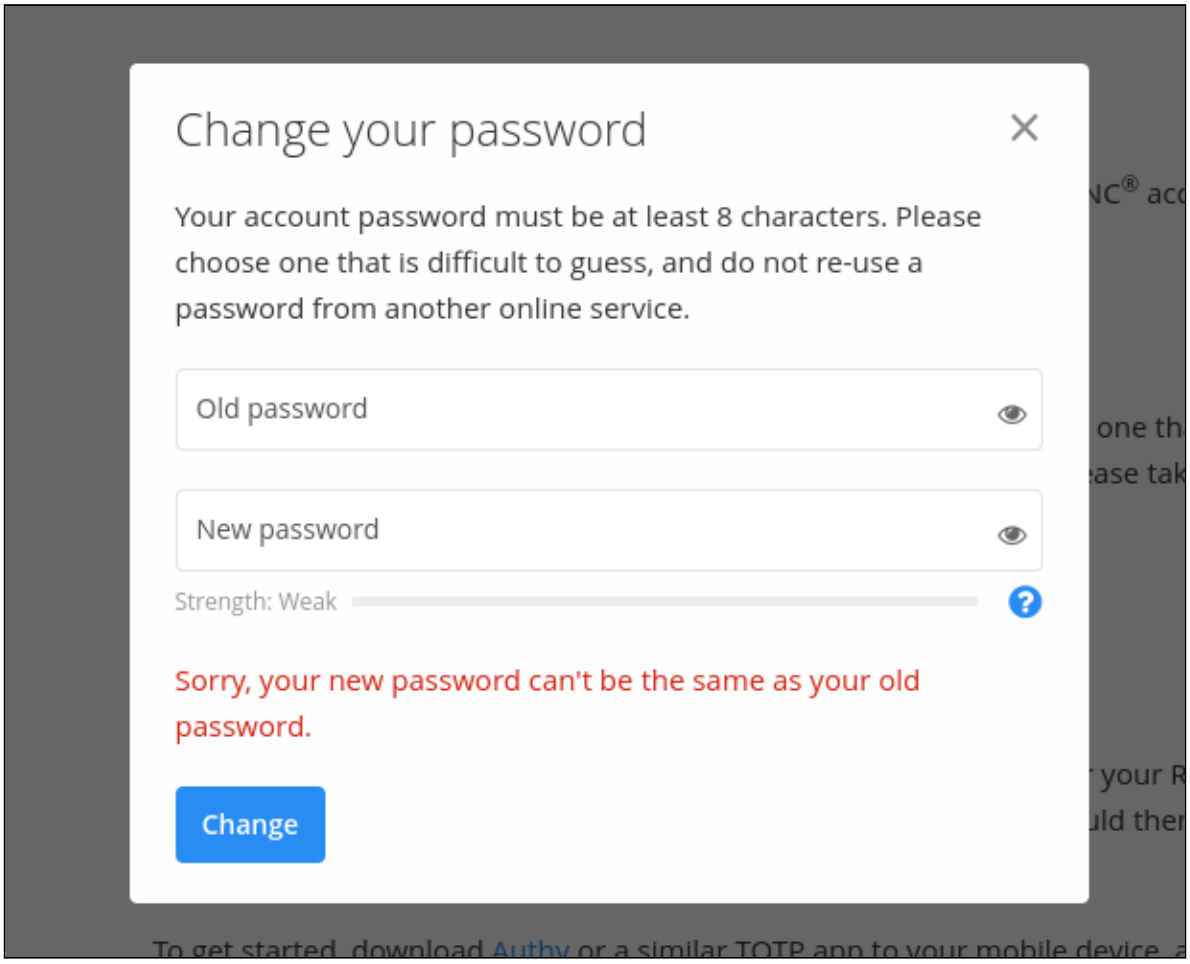

Figure 1: Only the password change functionality prevented password reuse

However, if using the Forgotten Password mechanism (accessible from the Log In page), a user could set their new password to be that of their original password.

Recommendation

Ensure that a suitably strong password policy is in place, commensurate with any defined policies for the application, system, or organisation.[49] [50] [51]

Passwords should be at least 10 characters long, and should be forced to include at least one upper case and one lower case letter, at least one special character and at least one digit. However, consideration could be given to relaxing password complexity in favour of a higher minimum length, providing that suitable guidance is given. This is because an examination of any large scale password dump will show that the majority of users choose a password which is in line with the bare minimum required by a policy but is nevertheless weak. Therefore, any technical controls in this area should also be supported by efforts to educate users, both on the reasons for the policy and with practical tips for the creation of secure passwords.

For administrator or more highly privileged accounts, a minimum length of 14 characters is typically recommended, with an enforced complexity at least equal to that set out above.

49. CWE-521: Weak Password Requirements:https://cwe.mitre.org/data/definitions/521.html
50. UK Government password guidance:https://www.ncsc.gov.uk/collection/passwords?curPage=/collection/passwords/updating-your-approach
51. OWASP Guidance:https://cheatsheetseries.owasp.org/

Other defences to consider include:

- Detecting and responding to automated password attacks (rate limit controls were observed that temporarily blocked brute-force behaviour, which appeared based on user's IP address)
- Blacklisting variations on common passwords, such as usernames, the application or the organisation (the password complexity estimator was providing such recommendations with respect to common passwords)
- Monitoring for unusual activity
- Making users aware of the last login event and encouraging them to report anything suspicious (it was noted that the application alerted users to log in attempts from a new IP address, which required user authorisation to proceed)

Furthermore, the RealVNC Portal provided users with the option to use multi-factor authentication (MFA).

Location

- https://s-manage.realvnc.com

Info

Weak TLS Cipher Suite Configuration

Overall Risk	Informational	**Finding ID**	NCC-E029530-UYE
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Configuration
		Status	New

Description

Some cipher suites supported by two of the hosts in scope were not sufficiently cryptographically secure and, as a result, cannot provide as much protection against brute-force decryption when compared to more modern cipher suites, should the traffic be captured.

The following cipher suites were supported, with the weak ciphers[52] highlighted in yellow. Note that the weak ciphers were *not* the preferred option.

```
TLSv1.2 (server order -- server prioritizes ChaCha ciphers when preferred by clients)
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256

TLSv1.3 (no server order, thus listed by strength)
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
```

Recommendation

Consult the server's documentation to disable weak cipher suites. Follow Mozilla's recommendation[53] for more guidance on general configuration of TLS. Mozilla's SSL Configuration Generator[54] provides a straightforward way to generate secure configuration for many common servers.

52. TLS Ciphersuite Search: https://ciphersuite.info/
53. Mozilla - Server Side TLS: https://wiki.mozilla.org/Security/Server_Side_TLS
54. Mozilla - SSL Configuration Generator: https://ssl-config.mozilla.org/

Location

- https://s-manage.realvnc.com

Info

Third-Party Script Included Without Subresource Integrity Hash

Overall Risk	Informational	**Finding ID**	NCC-E029530-3UM
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Other
		Status	New

Description

The Portal web application used JavaScript hosted by multiple third parties. This creates the risk that a compromise of the third party script host could result in a compromise of the application's users. Specifically, if an attacker compromises the third party host, they could replace the script with a malicious script that completely controls user accounts. Third party JavaScript has been documented as source of site compromise in the past.[55]

In order to mitigate this risk, Subresource Integrity (SRI)[56] was introduced as a browser feature in most major browsers.[57] This feature allows web applications to specify a hash of a script included with a `<script>` tag in order to verify the file has not been modified. Unfortunately, this feature has only received limited support from the vendors who most commonly provide hosted JavaScript. If the vendor does not support SRI, then the only choices may be to keep the functionality as is, or to remove the script and associated functionality.

The following external scripts were referenced:

- https://cdn.cookielaw.org/scripttemplates/otSDKStub.js
- https://static.zuora.com/Resources/libs/hosted/1.3.1/zuora-min.js
- https://www.paypalobjects.com/api/checkout.js

This issue can be observed by simply visiting an affected URL using a modern browser. View the HTML source of the page, paying attention to HTML script tags which have a `src` attribute.

Recommendation

Ideally, active content such as JavaScript, CSS, HTML, Java or Flash code should be hosted locally, rather than be included from third party hosts. If external hosting is preferred – usually for the performance gains delivered by content delivery networks (CDNs) – it is recommended that only reputable third parties are used and that, in the case of script and CSS files, the SRI attribute is added to force an integrity check. SRI specifies an encoded hash of the expected file, which conforming browsers will verify; for example:

```
<script src="//some.other.site.com/jquery/jquery.min.js" integrity="sha384-I6F5OKECLVtK/
↪BL+8iSLDEHowSAfUo76ZL9+kGAgTRdiByINKJaqTPH/QVNS1VDb" crossorigin="anonymous"></script>
```

55. The JavaScript Supply Chain Paradox: SRI, CSP and Trust in Third Party Libraries: https://www.troyhunt.com/the-javascript-supply-chain-paradox-sri-csp-and-trust-in-third-party-libraries/
56. Mozilla - Subresource Integrity (SRI): https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
57. Can I use - Subresource Integrity: https://caniuse.com/#feat=subresource-integrity

In this case, should the hash of the file received by the browser from the third party not match the value specified by the first party, the script will not be loaded. For more information on SRI implementation and browser support, see the footnotes, but note that SRI:

- Will prove problematic with resources that change without notice (and therefore it may be preferable to reference a specific version rather than the 'latest' version)
- Requires the `crossorigin` attribute
- Cannot check the integrity of scripts that are loaded dynamically
- Provides no effective protection if the first party page is delivered over HTTP

Location

- https://s-manage.realvnc.com

Info

Account Takeover (ATO) Protection Recommendations

Overall Risk	Informational	**Finding ID**	NCC-E029530-TDJ
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Authentication
		Status	New

Description

The Portal web application implemented a multi-layered defence against account takeover, including multi-factor authentication (MFA), and requiring user validation when accessing the application from a new IP address. The application also implemented rate limiting controls, which helped reduce the effectiveness of brute-force attacks, by temporarily blocking malicious activity based on the originating IP address. The security posture can be strengthened by implementing the additional measures outlined below.

The application did not temporarily lock out or alert users when multiple failed login attempts were made. Note that this issue in combination with finding "Password Policy and Implementation Recommendations" left the portal more vulnerable to password guessing attacks, as users could set weak or common passwords.

In the example that follows, a brute-force password guessing attack was conducted. The attack was configured using a slow password guess rate, which made one login attempt every five seconds. Following 53 incorrect login attempts, the application temporarily blocked the attack based on the attacker's IP address:

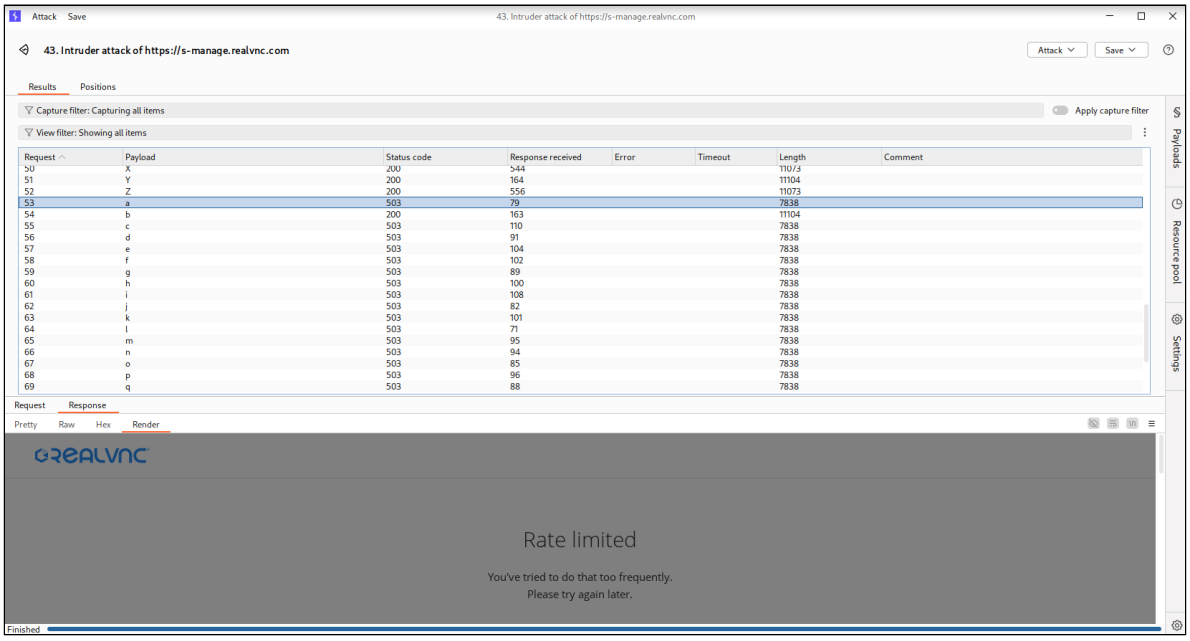

Figure 2: Encountering rate limit controls during a brute-force password guessing attack

The attack was continued from a new IP address (in this example, switching from one NCC Group VPN to another), and in this contrived example, the victim's password was identified

(see row 11) following approximately 64 guesses. However, the credential-based attack was hindered as the user was set up with MFA (which was an optional setting):

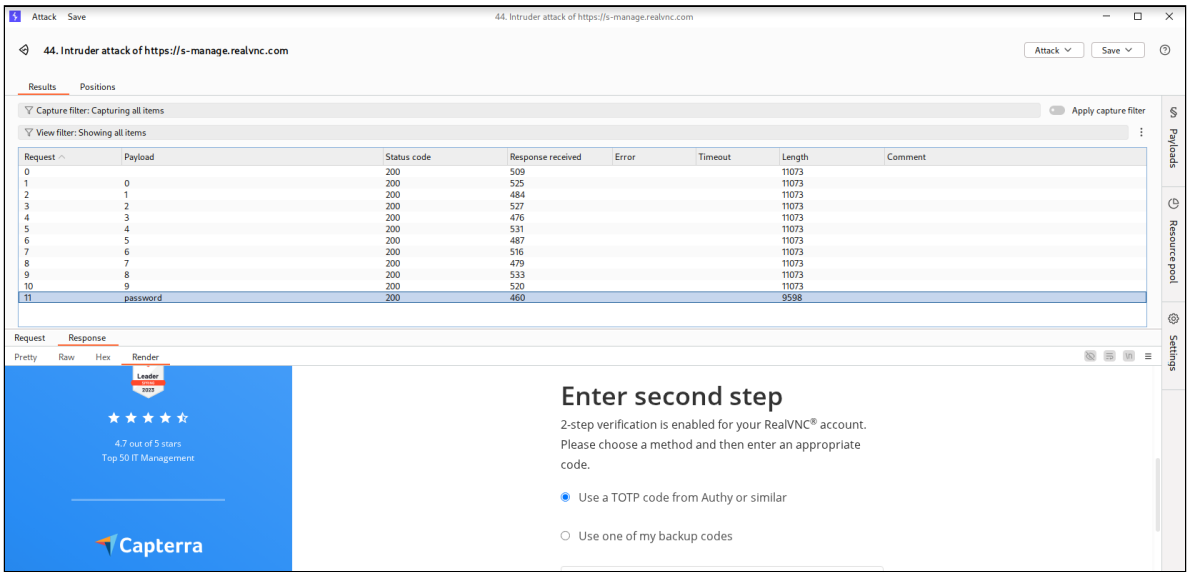

Figure 3: Side-stepping rate limit controls by using a different IP address

The victim received no alert about repeated failed login attempts, which might have encouraged enabling MFA. Furthermore, there was no evidence to suggest that the user was locked out from their account. The application identified the malicious activity and blocked the attacking IP address, which was side-stepped by changing IP addresses. An exponential or temporary account lockout would further hinder the attack, preventing continuation even if the attacker changed IP addresses.

Recommendation

Evaluate the following additional recommendations as components of a strong abuse protection system:[58] [59]

- Proactively monitor and alert on abuse signals such as multiple failed logins
- Implement a temporary lockout policy that automatically unlock the affected accounts after a period. Security best practice is to lock accounts for increasing periods following subsequent failed attempts to change the account's password (for example a third invalid attempt leads to a five-minute lockout, a sixth 10 minutes, ninth 15 minutes and so on).[60]

Location

- https://s-manage.realvnc.com

58. Elie Bursztein - Account protections. A Google Perspective: https://elie.net/talk/account-protections-a-google-perspective
59. Ryan McGeehan - Account Takeover (ATO) Checklist: https://github.com/magoo/ato-checklist
60. OWASP - Exponential / Temporary Lockout: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#account-lockout

Info

Wildcard SSL Certificate in Use

Overall Risk	Informational	**Finding ID**	NCC-E029530-6AJ
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Cryptography
		Status	New

Description

The Portal's API host used a wildcard SSL certificate. 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 was found:

```
SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.services.vnc.com
Altnames: DNS:*.services.vnc.com, DNS:services.vnc.com
Issuer:   DigiCert Global G2 TLS RSA SHA256 2020 CA1

Not valid before: Oct 17 00:00:00 2025 GMT
Not valid after:  Nov 17 23:59:59 2026 GMT
```

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.

If the wildcard certificate is used on any service that allows SSLv2 connections, then this service may be vulnerable to the DROWN attack.

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.[61] [62]

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

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

Location

- https://s-connect-api.services.vnc.com

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

Info

Password Reset Token Recommendations

Overall Risk	Informational	**Finding ID**	NCC-E029530-YFE
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	Low	**Category**	Authentication
		Status	New

Description

When performing a password reset (forgotten password) on the Portal web application, a token was issued via email, which allowed the user to change the password for the account associated with the reset token. Although good security practices were observed (for example, password reset tokens could not be reused once used), the security posture could be strengthened by implementing the additional measures outlined below.

The first observation was regarding the reset token's longevity. If the token was not used, it would automatically expire after a 24-hour period (identified from Base64 decoding the JSON Web Token [JWT] reset link). Instead, it is recommended that such tokens automatically expire after a relatively short period to minimise risk from intercepted or disclosed tokens. The OWASP recommendation is to limit this period to no more than one hour.[63] In addition, subsequent password reset requests did not invalidate all previously issued reset tokens for the same user account. However, the action of setting a new password did invalidate all other issued reset tokens.

The password reset page also disclosed the user's email address, as demonstrated below, rather than prompting the user to provide the email address associated with the account during the password reset process in order to successfully perform a reset. As a result, an attacker would not need to guess the user's username in order to take over the account.

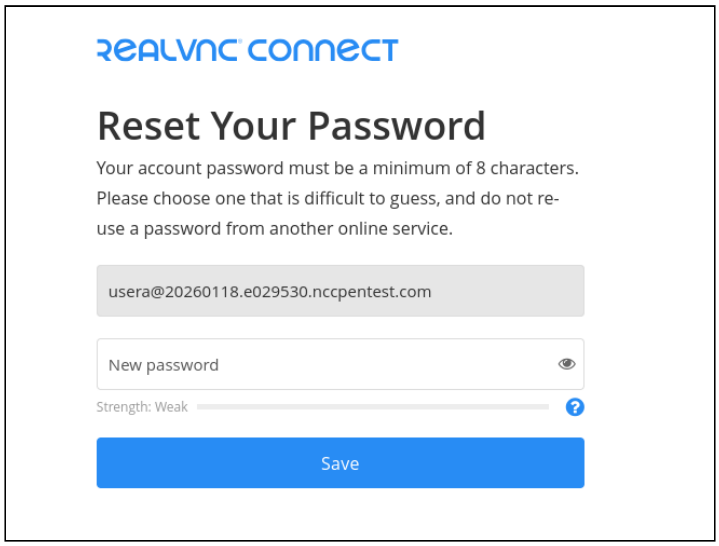

Figure 4: The reset password journey disclosed the user's email address

63. OWASP - Testing for Weak Password Change or Reset Functionalities: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/09-Testing_for_Weak_Password_Change_or_Reset_Functionalities

The risk associated with this issue was reduced due to the Portal application notifying users about their account password change, thus raising awareness of any malicious activity. As such, this issue has been reported for informational purposes only.

Recommendation

Reset token links should be time limited, but exactly how long is appropriate will depend on the site. Some systems allow up to 24 hours, but this is considered the upper limit.[64]

Log all password reset attempts that are rejected due to the use of an expired token.

Location

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

64. Forgot Password Cheat Sheet - OWASP: https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html

Info

Session Invalidation Observation

Overall Risk	Informational	**Finding ID**	NCC-E029530-AAU
Impact	Low	**Component**	Portal Web Application Assessment
Exploitability	None	**Category**	Session Management
		Status	New

Description

The Portal web application allowed users to change their passwords and log out, though in both cases session termination was subject to a very minor delay. Instead of immediately terminating the user's session (for example, by invalidating the session upon change of password), the user's session expired by the `exp` parameter. However, with an expiration period of only 5 minutes, the risk of prolonged use of a compromised session token was significantly reduced. As such, this issue has been raised as informational and reported for awareness.

An example of this behaviour is demonstrated below for log out. The first request is of the user initiating log out:

Request

While the request included a substantial number of cookies (removed in this example for brevity), the session was managed by the cookie named `title`, which held a JSON Web Token (JWT). Its `exp` value was `Fri 12 December 2025 14:26:44 UTC`:

```
POST /en/auth/sign_out?ts=a HTTP/2
Host: s-manage.realvnc.com
Cookie: token=eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJNeHhVQTN0VHdiUHpWZmhlV3ZRIiwicmVuZXdhbFNlcSI6MCwi
↳ c2Vzc2lvbklkIjoiTXh4VVNRZ1lYblg5RHlXaWZLeSIsIl9raWQiOiJzZXNzaW9uLWludGVybmFsIiwiMmZhIjpmYWxzZ
↳ SwiX2l2IjoiNGRzc1BCUDZjbS9meW81dFkraW1NZz09IiwicmVuZXdhbEV4cGlyeVRpbWUiOjE3NjU1NTExMDQsInJlcX
↳ Vlc3RUaW1lIjoxNzY1NTQ5MzA0LCJhdWQiOiJzZXNzaW9uIiwiX2VuY3J5cHRlZCI6InkxQXBjdEVsazQ5dDhZL1FKZjF
↳ xRWl2WUZoMjFaNWV5YmVCWlp1SERHQVN3Sm1iSk1zZVNmWVYvcU1IbWNBNWRCd3o5eFN5bnYzejhjRGlqa0dTUWVyd2Nn
↳ Q00wMk1RcFdHNVl2WnFDR2phUkM5VjJOamp3T1J3S3FDZEJxeGp5S3BIckxXeWowWjFxR2dCdHNqRjFPNVE9Iiwic2Nvc
↳ GUiOiI0IiwiZXhwIjoxNzY1NTQ5NjA0LCJpYXQiOjE3NjU1NDkzMDR9.g4_4NjOc05GYIAvB7S-
↳ chw5_ePrvPVHgmey89Stf41u6ppVlVURmLSdNu9riZRugS_q9TZqMwSqPnTLAwHtjuljfz6YX5ubRlvIWUF4kWP-2mATq
↳ AlC3GAmsBsThAOJjKeVNlFPOatY7Cr4W_V841IMyQ6w6_Bjku1ueE77NzhQy6v8LcKTvAxe2GQ0nGCPmLDWf_v7dT95oY
↳ pRkRvZ0Ugx_Md9Ww2nSgkHWisyiDPCwNwOcZQJYX8o5G6_wVfslZmjM8OpG6YJ4oxsVmvL0OXViBaIzImN9g8CX9AH9a2
↳ O0st2W1yflfG3F1-lPz1rQMOWQWUGon8Uo29r3HLgP8A;
{REMOVED FOR BREVITY}
```

The server responded by clearing the cookies from the user's browser:

Response

```
HTTP/2 302 Found
Date: Fri, 12 Dec 2025 14:22:26 GMT
Set-Cookie: renewal_expiry=1765551104; Path=/; secure
Set-Cookie: session=_WxEzvqoNHtH2-
↳ rhaYuz62onesgX9qIUSF_wRfAdZtUrd26YPKTx7VF09t3Z8fI9PAdx6E02x9PqIQDheSYyl1sxNzY1NTQ5MzQ2LCAxNzY
↳ 1MzYwMzg1LjI1MjMyNDYsIHsiX2NzcmZ0XyI6ICJmZDlmNDgxZTRhYTQ3M2ZhNjI3MTRiMGY5NjZhZjYzOTJmMzc2YmY1
↳ IiwgInRyaWFsX3N0YXRlIjogImEiLCAic3VzcGVuc2lvbl9kYXRhIjogeyJ0ZWFtIjogImNkb09VM3MzQllKc2RUVlhxV
↳ XkiLCAibXNwIjogZmFsc2V9fV0; Path=/; secure; HttpOnly; SameSite=Lax
```

```
Set-Cookie: token=; Max-Age=0; Path=/; expires=Wed, 31-Dec-97 23:59:59 GMT
Set-Cookie: plan-PKG0004-D=; Domain=.realvnc.com; Max-Age=0; Path=/; expires=Wed, 31-Dec-97
↳ 23:59:59 GMT
Set-Cookie: License_type=; Domain=.realvnc.com; Max-Age=0; Path=/; expires=Wed, 31-Dec-97
↳ 23:59:59 GMT
{REMOVED FOR BREVITY}
```

However, the session token remained valid and was successfully used to query the Profile page, returning an authenticated response:

Request

```
GET /en/profile?ts=a HTTP/2
Host: s-manage.realvnc.com
Cookie: token=eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJNeHhVQTN0VHdiUHpWZmhlV3ZRIiwicmVuZXdhbFNlcSI6MCwi
↳ c2Vzc2lvbklkIjoiTXh4VVNRZ1lYblg5RHlXaWZLeSIsIl9raWQiOiJzZXNzaW9uLWludGVybmFsIiwiMmZhIjpmYWxzZ
↳ SwiX2l2IjoiNGRzc1BCUDZjbS9meW81dFkraW1NZz09IiwicmVuZXdhbEV4cGlyeVRpbWUiOjE3NjU1NTExMDQsInJlcX
↳ Vlc3RUaW1lIjoxNzY1NTQ5MzA0LCJhdWQiOiJzZXNzaW9uIiwiX2VuY3J5cHRlZCI6InkxQXBjdEVsazQ5dDhZL1FKZjF
↳ xRWl2WUZoMjFaNWV5YmVCWlp1SERHQVN3Sm1iSk1zZVNmWVYvcU1IbWNBNWRCd3o5eFN5bnYzejhjRGlqa0dTUWVyd2Nn
↳ Q00wMk1RcFdHNVl2WnFDR2phUkM5VjJOamp3T1J3S3FDZEJxeGp5S3BIckxXeWowWjFxR2dCdHNqRjFPNVE9Iiwic2Nvc
↳ GUiOiI0IiwiZXhwIjoxNzY1NTQ5NjA0LCJpYXQiOjE3NjU1NDkzMDR9.g4_4NjOc05GYIAvB7S-
↳ chw5_ePrvPVHgmey89Stf41u6ppVlVURmLSdNu9riZRugS_q9TZqMwSqPnTLAwHtjuljfz6YX5ubRlvIWUF4kWP-2mATq
↳ AlC3GAmsBsThAOJjKeVNlFPOatY7Cr4W_V841IMyQ6w6_Bjku1ueE77NzhQy6v8LcKTvAxe2GQ0nGCPmLDWf_v7dT95oY
↳ pRkRvZ0Ugx_Md9Ww2nSgkHWisyiDPCwNwOcZQJYX8o5G6_wVfslZmjM8OpG6YJ4oxsVmvL0OXViBaIzImN9g8CX9AH9a2
↳ O0st2W1yflfG3F1-lPz1rQMOWQWUGon8Uo29r3HLgP8A;
```

Response

```
HTTP/2 200 OK
Date: Fri, 12 Dec 2025 14:26:02 GMT
{REMOVED FOR BREVITY}

<dd id="displayed-email" class="small-12 medium-10 columns">
        managerb@20260118.e029530.nccpentest.com
</dd>
```

The token was properly rejected upon expiration:

Response

```
HTTP/2 401 Unauthorized
Date: Fri, 12 Dec 2025 14:26:57 GMT
{REMOVED FOR BREVITY}
```

Recommendation

As JWTs are stateless, manual expiration is not possible. A common mitigation is the use of a token deny list. The application should be designed so that, upon logout, the active token is recorded in the deny list until expiry. Subsequent requests containing a token from this list should be rejected, with the user redirected to the login page.[65]

Location

- https://s-manage.realvnc.com

65. Revoking a JWT access token: https://authress.io/knowledge-base/academy/topics/invalidating-user-access#revoking-a-jwt-access-token