CCL SOLUTIONS GROUP

Heat Network Zoning

Web Application & API Penetration Testing Report

Client	ICS
Project	Heat Network Zoning
Reference	CS11675
Prepared for	Phil Slemmings
Author	Bianca Napoleonov
Testing Team	Bianca Napoleonov
Date	October 14, 2025
NCSC Reference Number:	CK2025-V9N5M-3634

Assured Service Provider

in association with National Cyber Security Centre

CHECK Penetration Testing

CCL SOLUTIONS GROUP

Contents

1. Document Control

1.1. Document Details

Title	Heat Network Zoning
Author	Bianca Napoleonov
Version	1.0
Date	October 14, 2025
Document Reference	CS11675
Status	Definitive

1.2. Revision History

Version	Date	Author	Summary of Changes
0.1	13/10/2025	Bianca Napoleonov	Initial Draft
0.2	14/10/2025	Niall Aiken	QA
1.0	14/10/2025	Niall Aiken	Definitive

1.3. Distribution

Name	Email	Organisation
Phil Slemmings	phil.slemmings@tpximpact.com	ICS

2. Executive Summary

CCL Solutions Group carried out a Web Application and API security assessment. The test took place between 06/10/2025 and 09/10/2025. The testing was carried out by the consultant named in Appendix A. The customer contact of this engagement was Phil Slemmings(phil.slemmings@tpximpact.com).

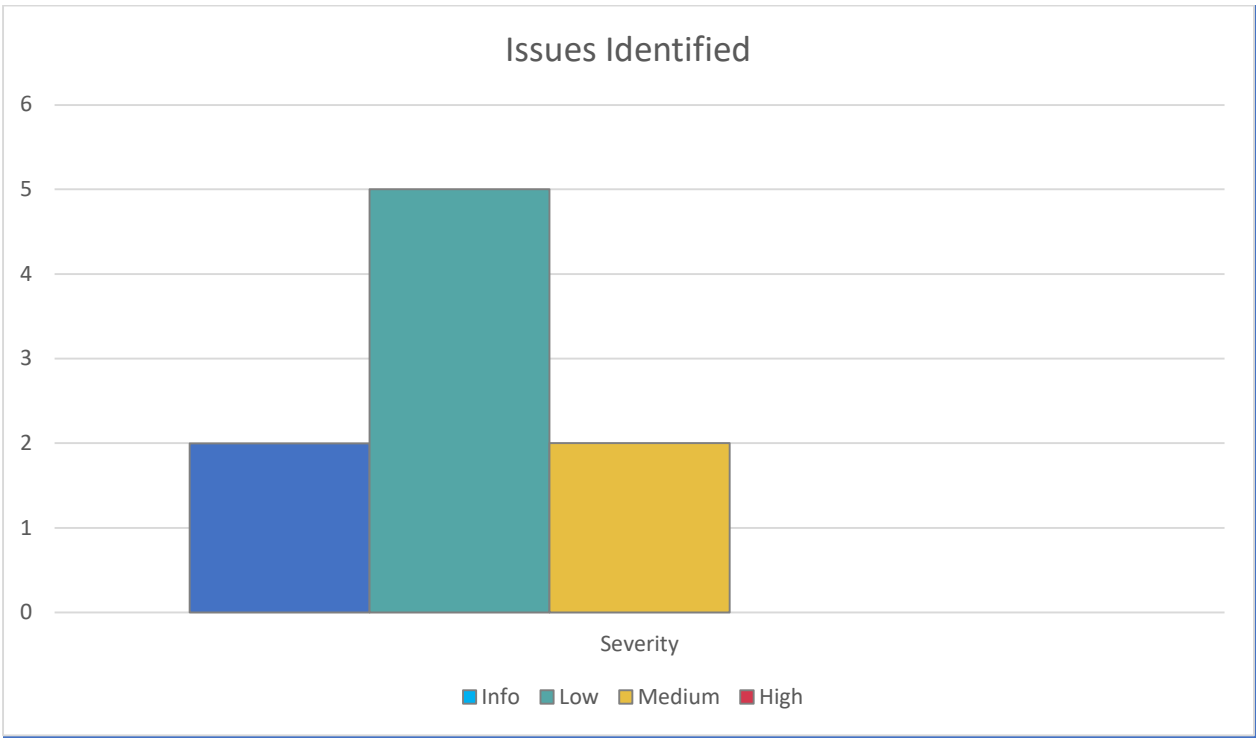
The assessment identified nine findings across the web application, ranging from medium-risk security misconfigurations to informational items requiring attention. Whilst no critical or high-risk vulnerabilities were discovered, several areas require remediation to strengthen the overall security posture and improve defensive capabilities.

The application exhibited several security misconfigurations that collectively weaken its defensive posture. Key concerns include the absence of rate limiting controls that could facilitate denial of service attacks, missing Strict Transport Security headers that compromise secure communications, and outdated cipher suites vulnerable to cryptographic attacks.

Additional issues were identified around content sniffing protection, input validation controls, and session timeout configurations. Furthermore, the platform lacks proper user intent verification for destructive actions, potentially leading to accidental data loss and increased operational burden.

Two implementation considerations were identified that, whilst not direct security vulnerabilities, present operational and user experience implications. The application permits concurrent user sessions, which may weaken access control and session management. Additionally, certain HTTP headers disclose system information that could assist attackers in reconnaissance activities.

The identified vulnerabilities present no immediate risk to business operations; however, the cumulative effect of these misconfigurations could provide attackers with footholds for more sophisticated attacks.



3. Next Steps

The goals provided are set out to be suggestions and should be reviewed and fixed according to the risk posed to your business model.

Short Term Goals

- Implement rate limiting on the relevant endpoints to prevent service disruption attacks.
- Configure Strict Transport Security (HSTS) headers to enforce secure HTTPS connections.
- Enable content sniffing protection by setting appropriate X-Content-Type-Options headers.
- Remove or minimise information disclosure in HTTP response headers that reveal system details.

Medium Term Goals

- Add confirmation dialogs for all destructive actions to prevent accidental data deletion.
- Strengthen input validation across forms and user inputs to improve data integrity.
- Review and adjust session timeout configurations to balance security with user experience.
- Update SSL cipher suites to remove weak CBC ciphers and implement modern encryption standards.

Long Term Goals

- Evaluate concurrent session management policies and implement controls if required by business needs.

4. Technical Information

4.1. Background

CCL (Solutions) Group Ltd. were engaged by ICS to assess the security of Heat Network Zoning Web Application, to support their ongoing accreditation requirements. This was conducted adhering to the below scope in accordance with the CCL Security Testing Methodology (DOC-10001).

4.2. Scope

Below is the scope information provided to the security consultants for the penetration testing:

Host	Description
www.heat-network-zoning.data.gov.uk	Heat Network Zoning User and Admin portal

4.2.1. User Accounts

User accounts were provided for all external applications within the scope of the engagement with multiple levels of access.

Username	Description
Bianca.Napoleonov+user@cclsolutionsgroup.com	Standard user
Bianca.Napoleonov+admin@cclsolutionsgroup.com	Admin user

4.3. Rules of Engagement

The penetration test was performed in line with the following rules of engagement:

- Grey box testing methodology was used.
- The engagement was conducted remotely.

4.4. Limitations

Some application features required additional refinement, causing slight schedule delays. The following endpoints were not tested due to current implementation limitations.

/api/zonestatestage

/api/zone/zone_id

5. Findings Summary

5.1. Web Application Testing Summary

Reference	Vulnerability	Severity	Remediation
1	**Lack of Rate Limiting** The application lacks rate limiting, allowing users or attackers to send an excessive number of requests in a short period without restriction.	Medium	Implement rate limiting which involves controlling the number of requests that clients can make within a certain time frame.
2	**Strict Transport Security Header Not Configured** The HTTP Strict Transport Security (HSTS) header was not configured on the web server.	Medium	The HSTS header should be added to all applications to ensure all communications are encrypted.
3	**Content Sniffing not Disabled** The X-Content-Type-Options: nosniff header was not present in all server's responses.	Low	Set the header at least in all responses which contain user input.
4	**Insufficient Input Validation** Insufficient user input validation for parameters such as email, role, etc., allowed malicious data to be inserted which could lead to further vulnerabilities.	Low	To address the issue of insufficient input validation, implement robust server-side validation to ensure all input conforms to expected formats, types, and ranges before processing.
5	**Insufficient User Intent Verification for Data Deletion** The application allows users to permanently delete data without presenting a confirmation dialog or requiring explicit user intent verification.	Low	Implement confirmation dialogs for all destructive actions or consider soft delete with undo functionality.
6	**SSL Weak Cipher Suites (CBC)** The application's TLS configuration used Cipher Block Chaining (CBC) ciphers which are vulnerable to oracle padding attacks.	Low	Weak methods of encryption should be disabled to ensure only secure cipher suites are used.
7	**Excessive Session Timeout Configured** The application was found to have an excessive session timeout configured.	Low	Implement a session timeout policy that terminates sessions after a defined period of inactivity. Session timeouts should be set to as minimal a value as possible depending on the context of the application.

8	**Concurrent Logins Supported** The application supports concurrent logins as the same user.	**Informational**	Concurrent logins should be prevented, particularly for privileged accounts.
9	**Information Disclosure via HTTP Header** The application was found to reveal the web framework supporting the service within the HTTP banners.	**Informational**	The "X-Powered-By: " banner should not be returned by the server.

6. Web Application Testing

This section details the Web Application findings that were identified during the testing engagement.

6.1. Lack of Rate Limiting

Severity	Medium
Impact	3
Likelihood	3
Fix Effort	Intermediate
Status	Ongoing
Reference	1

6.1.1. Summary

Rate-limiting is used in web applications and APIs to limit the number of requests that can be made to the endpoint, once this limit is reached service should be denied to the user. With a lack of rate-limiting an attacker is able to repeat requests an unlimited number of times leading to an associated drain on the resources of the server, potentially resulting in a denial-of-service (DoS) attack.

6.1.2. Technical Information

It was noted during testing that the /api directory lacked rate limiting on its endpoints, allowing large number of requests to be sent to the server. This caused the service to become unavailable (DoS).

Request:

```
PUT /api/managezone/00nw1qpwuXJ-0 HTTP/2
Host: www.heat-network-zoning.data.gov.uk
Cookie: arcgis_token=mzFcMRqhxzPAoRJavp2MJkRRNOon2PShQlI7pGdeXz6ClZ-
99WTmts7kMeAjdxYYxOK3kXXoLxl1kjEvwybwa3JfczHhMOaylNPu3DOIFq_gWUCIWb-W6al6YthQfttuFpy-
Z_w9nGP2gpZeVDaTljxbFSNfsDNyWUisOtvDLRLMqhGbDeQPFV0SdcUc0pQHdbBGhD2mS0JdSFRwI_YC9A..;
arcgis_token_expiry=1760352258040; __Secure-next-auth.session-
token=eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIn0..Q5AYWiulc-0VrpfW.ZTz_qFPFDhdIauyGAwqb-6EKgpSr49D_2buv-
3sgy8Oq8WbV9p5Vq1ML7iVqlBcqV4I1tGhaJ4VrXjDqZVOFSvoAKt_ixYIoBVwKwasmgRCjebylLcarYdJxnijrgHdnqaIw63NLonoF4EgYgWNU3
ITytM6kTB4yo00lM4stnT4eynouJzU32hUcXTAOwTnpOCP4CRJmDiMzGcWs56cNAjYS87PACF5n5zeEh5N-
a6idhjyGc2_e9dpJiiIS1lWphi9WF6yPNT3j-KvelLGqQnBunA6RF95rmptayDPBduoXaG0.ancQZKzS7QR8F4-vR_AeSA
Content-Length: 820
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
Accept: */*
Origin: https://www.heat-network-zoning.data.gov.uk
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.heat-network-zoning.data.gov.uk/manage-zones/00nw1qpwuXJ-0
```

```
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
{"id":904,"zone_id":"00nw1qpwuXJ-2","fid":"906","state":"Opportunity area","name":"None
assigned","state_id":1,"coordinators":[{"id":714,"name":"Pen
Test","role":"test","contact_email":"bianca.napoleonov+coord@cclsolutionsgroup.com","organisation":"CCL","zone_c
oordinator_lead":false}],"notes":[{
--redacted--
```

Response:

```
HTTP/2 500 Internal Server Error
Date: Thu, 09 Oct 2025 14:17:37 GMT
Content-Type: application/json
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
{"error":"Error updating zone"}
```

#	Time	Method	Host	Path
7872	15:17:40 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7871	15:17:40 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7870	15:17:40 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7869	15:17:40 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7868	15:17:39 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7867	15:17:39 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7866	15:17:39 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7865	15:17:39 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7864	15:17:39 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7863	15:17:38 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7862	15:17:38 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7861	15:17:38 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7860	15:17:38 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7859	15:17:37 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7858	15:17:37 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7857	15:17:37 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7856	15:17:37 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7855	15:17:37 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7854	15:17:36 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7853	15:17:36 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7852	15:17:36 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7851	15:17:36 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7850	15:17:35 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7849	15:17:35 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7848	15:17:35 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7847	15:17:35 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7846	15:17:35 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7845	15:17:35 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7844	15:17:34 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7843	15:17:34 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7842	15:17:34 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7841	15:17:34 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7840	15:17:34 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7839	15:17:33 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7838	15:17:33 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7837	15:17:33 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7836	15:17:33 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7835	15:17:33 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7834	15:17:32 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7833	15:17:32 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7832	15:17:32 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7831	15:17:32 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0
7830	15:17:32 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0_backup
7829	15:17:31 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0_bak
7828	15:17:31 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0_old
7827	15:17:31 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/backup_00nw1qpwuXJ-0
7826	15:17:31 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-01
7825	15:17:31 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/bak_00nw1qpwuXJ-0
7824	15:17:31 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/00nw1qpwuXJ-0%20-%20...
7823	15:17:30 9 Oct 2025	PUT	www.heat-network-zoning.data.gov.uk	/api/managezone/old_00nw1qpwuXJ-0

Figure 1 - Excessive number of requests in a short period.

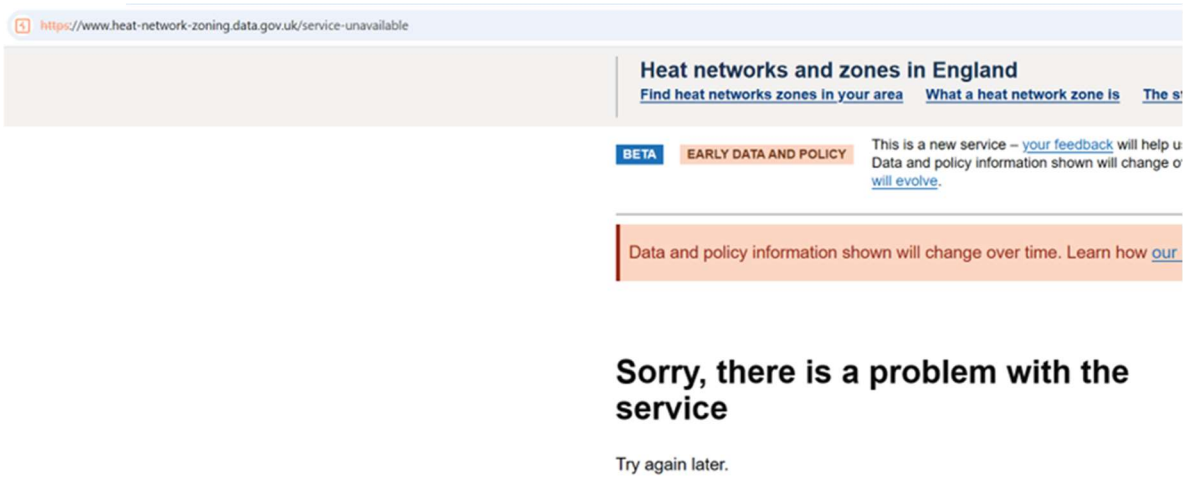


Figure 2 - Service unavailable due to large number of requests allowed.

6.1.3. Recommendations

Implementing rate limiting on an API involves controlling the number of requests that clients can make within a certain time frame. This helps prevent abuse, misuse, and denial-of-service attacks. There are a number of methods for introducing rate limiting to an application, these include:

- Token Bucket: Clients consume tokens at a fixed rate, and requests are only served if there are available tokens.
- Fixed Window: Counts the number of requests within a fixed time window (e.g., per second, per minute).
- Sliding Window: Maintains a rolling window of requests within a specified time period.

The chosen method should be enforced by the web server and when the rate limit is exceeded an appropriate error code should be provided to the user, for example "HTTP status code 429 - Too Many Requests.

6.1.4. References

https://www.owasp.org/index.php/Denial_of_Service

https://www.cloudflare.com/learning/bots/what-is-rate-limiting/

6.1.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.2. Strict Transport Security Header Not Configured

Severity	Medium
Impact	2
Likelihood	3
Fix Effort	Easy
Status	Ongoing
Reference	2

6.2.1. Summary

The HTTP Strict Transport Security (HSTS) header was not configured on the web server. This is a security header which can be sent by a web server to inform the browser to only communicate over HTTPS. Once the browser has received this header it will restrict the user from being able to access HTTP content on the same domain ensuring that all communications are encrypted. Once the configured max-age time period has expired the browser will allow clear-text HTTP communications with the domain again. The max-age countdown resets each time a response is received containing the HSTS header.

6.2.2. Technical Information

The Strict-Transport-Security header was not present in any responses from the web server. Below is an example response for the /admin section of the application.

Request:

```
GET /admin HTTP/2
Host: www.heat-network-zoning.data.gov.uk
Cookie: __Host-next-auth.csrf-
token=89aedf52b0df7371dc63868087375b0fca995d15705665043ab9b1119090e7d8%7Cee7edaddcddce2dd324465b978f42ad38a06aa3
9a9d978c409108ee0a91826b5; __Secure-next-auth.callback-url=https%3A%2F%2Fwww.heat-network-zoning.data.gov.uk%2F;
arcgis_token=mzFcMRqhxzPAoRJavp2MJkRRNOon2PShQlI7pGdeXz6ClZ-
99WTmts7kMeAjdxYYxOK3kXXoLxl1kjEvwybwa3JfczHhMOaylNPu3DOIFq_gWUCIWb-W6al6YthQfttuFpy-
Z_w9nGP2gpZeVDaTljxbFSNfsDNyWUisOtvDLRLMqhGbDeQPFV0SdcUc0pQHdbBGhD2mS0JdSFRwI_YC9A..;
arcgis_token_expiry=1760352258040; __Secure-next-auth.session-
token=eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIn0..wBnPR6w3RMI0SGfQ.R7Cfeay379HpiazosIGZ50-
HkCHHBziKFgQHokyYk8lOwZPMC94RJiNEuDZ5IiIGSqTIeZnmwLkE6r4qwAfmywPoxED5j_63oflygodREIzTorxBSXvV3vyCmlH3kdqXx8Auk45
bbjTjxZ4DSirKzAUIq2UBvkY8qMoUu41jF4-
RBXBpahJHN5uQfqNhhEmCOSl0CeuqA4wVHs5VM1kl0uHaREkEfHXdq6NvD844ztxfM73fYU_hza30Jg8UIRUAy9b5HXNiH__RoQXycbiOZU3dUsl
P5A4l9epehcDQs3UrUzo.xr6y4FK8E6IXddgeRTLyzQ
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
```

```
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response:

```
HTTP/2 200 OK
Date: Tue, 07 Oct 2025 11:05:58 GMT
Content-Type: text/html; charset=utf-8
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding
X-Nextjs-Cache: HIT
X-Powered-By: Next.js
Cache-Control: s-maxage=31536000, stale-while-revalidate
Etag: "xexpnmf5s7i15"
<!DOCTYPE html><html lang="en">
--redacted--
```

6.2.3. Recommendations

The HSTS header should be added to all applications to ensure all communications are encrypted. As an example, the following header would enforce HTTPS for one year: `Strict-Transport-Security: max-age=31536000`

Note: The max-age value is specified in seconds.

6.2.4. References

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

6.2.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.3. Content Sniffing not Disabled

Severity	Low
Impact	1
Likelihood	1
Fix Effort	Easy
Status	Ongoing
Reference	3

6.3.1. Summary

The X-Content-Type-Options response HTTP header is used by the server to indicate to the browsers that the MIME types advertised in the Content-Type headers should be followed and not guessed.

The lack of this header causes certain browsers to try to determine the content type and encoding of the response even when these properties are defined correctly. This can make the web application vulnerable against Cross-Site Scripting (XSS) attacks. E.g. the Internet Explorer and Safari treat responses with the content type text/plain as HTML, if they contain HTML tags.

6.3.2. Technical Information

The X-Content-Type-Options: nosniff header was not present in all server's responses. Below is an example response from /admin/zonestate:

Request:

```
GET /admin/zonestate?_rsc=1pazn HTTP/2
Host: www.heat-network-zoning.data.gov.uk
Cookie: __Host-next-auth.csrf-
token=89aedf52b0df7371dc63868087375b0fca995d15705665043ab9b1119090e7d8%7Cee7edaddcddce2dd324465b978f42ad38a06aa3
9a9d978c409108ee0a91826b5; __Secure-next-auth.callback-url=https%3A%2F%2Fwww.heat-network-zoning.data.gov.uk%2F;
arcgis_token=mzFcMRqhxzPAoRJavp2MJkRRNOon2PShQlI7pGdeXz6ClZ-
99WTmts7kMeAjdxYYxOK3kXXoLxl1kjEvwybwa3JfczHhMOaylNPu3DOIFq_gWUCIWb-W6al6YthQfttuFpy-
Z_w9nGP2gpZeVDaTljxbFSNfsDNyWUisOtvDLRLMqhGbDeQPFV0SdcUc0pQHdbBGhD2mS0JdSFRwI_YC9A..;
arcgis_token_expiry=1760352258040; __Secure-next-auth.session-
token=eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIn0..wBnPR6w3RMI0SGfQ.R7Cfeay379HpiazosIGZ50-
HkCHHBziKFgQHokyYk8lOwZPMC94RJiNEuDZ5IiIGSqTIeZnmwLkE6r4qwAfmywPoxED5j_63oflygodREIzTorxBSXvV3vyCmlH3kdqXx8Auk45
bbjTjxZ4DSirKzAUIq2UBvkY8qMoUu41jF4-
RBXBpahJHN5uQfqNhhEmCOSl0CeuqA4wVHs5VM1kl0uHaREkEfHXdq6NvD844ztxfM73fYU_hza30Jg8UIRUAy9b5HXNiH__RoQXycbiOZU3dUsl
P5A4l9epehcDQs3UrUzo.xr6y4FK8E6IXddgeRTLyzQ
Rsc: 1
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Next-Router-Prefetch: 1
Next-Router-State-Tree:
%5B%22%22%2C%7B%22children%22%3A%5B%22admin%22%2C%7B%22children%22%3A%5B%22__PAGE__%22%2C%7B%7D%2C%22%2Fadmin%22
%2C%22refresh%22%5D%7D%5D%7D%2Cnull%2Cnull%2Ctrue%5D
Next-Url: /admin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
```

```
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.heat-network-zoning.data.gov.uk/admin
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response:

```
HTTP/2 200 OK
Date: Tue, 07 Oct 2025 11:05:58 GMT
Content-Type: text/x-component
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding
X-Nextjs-Cache: HIT
Cache-Control: s-maxage=31536000, stale-while-revalidate
Etag: "wzl2dk3syzayu"
2:I[9107, --redacted--
```

6.3.3. Recommendations

Set the following HTTP header at least in all responses which contain user input:

`X-Content-Type-Options: nosniff`

6.3.4. References

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

6.3.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.4. Insufficient Input Validation

Severity	Low
Impact	1
Likelihood	2
Fix Effort	Intermediate
Status	Ongoing
Reference	4

6.4.1. Summary

Input validation is the testing of any input supplied by a user or application and prevents improperly formed data from entering an application. Input validation should happen as early as possible in the data flow, ideally as soon as the data is received. Failure to enforce sufficient input validation would enable an attacker to input malicious data which could lead to further vulnerabilities.

6.4.2. Technical Information

Insufficient user input validation for parameters such as email, role, etc., allowed malicious data to be inserted which could lead to further vulnerabilities.

Request:

```
PUT /api/managezone/00nw1qpwuXJ-0 HTTP/2
Host: www.heat-network-zoning.data.gov.uk
Cookie: arcgis_token=mzFcMRqhxzPAoRJavp2MJkRRNOon2PShQlI7pGdeXz6ClZ-
99WTmts7kMeAjdxYYxOK3kXXoLxl1kjEvwybwa3JfczHhMOaylNPu3DOIFq_gWUCIWb-W6al6YthQfttuFpy-
Z_w9nGP2gpZeVDaTljxbFSNfsDNyWUisOtvDLRLMqhGbDeQPFV0SdcUc0pQHdbBGhD2mS0JdSFRwI_YC9A..;
arcgis_token_expiry=1760352258040; __Secure-next-auth.session-
token=eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIn0..Q5AYWiulc-0VrpfW.ZTz_qFPFDhdIauyGAwqb-6EKgpSr49D_2buv-
3sgy8Oq8WbV9p5Vq1ML7iVqlBcqV4I1tGhaJ4VrXjDqZVOFSvoAKt_ixYIoBVwKwasmgRCjebylLcarYdJxnijrgHdnqaIw63NLonoF4EgYgWNU3
ITytM6kTB4yo00lM4stnT4eynouJzU32hUcXTAOwTnpOCP4CRJmDiMzGcWs56cNAjYS87PACF5n5zeEh5N-
a6idhjyGc2_e9dpJiiIS1lWphi9WF6yPNT3j-KvelLGqQnBunA6RF95rmptayDPBduoXaG0.ancQZKzS7QR8F4-vR_AeSA
Content-Length: 922
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36
Accept: */*
Origin: https://www.heat-network-zoning.data.gov.uk
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.heat-network-zoning.data.gov.uk/manage-zones/00nw1qpwuXJ-0
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
{"id":904,"zone_id":"00nw1qpwuXJ-2","fid":"906","state":"Opportunity area","name":"None
assigned","state_id":1,"coordinators":[{"id":714,"name":"Pen
Test","role":"test","contact_email":"bianca.napoleonov+coord@cclsolutionsgroup.com","organisation":"CCL","zone_c
oordinator_lead":false}],"notes":[{"id":null,"zoneId":904,"coordinatorId":714,"notes_title":"Opportunity area
```

```
'\"<>/;a,=-","notes_body":"'\";<>/\\asda","notes_zc_name":"Pen
Test","notes_zc_contact":"bianca.napoleonov+coord@cclsolutionsgroup.com","zone_reference_id":"00nw1qpwuXJ-
0","created_at":"2025-10-09T10:27:53.406Z","coordinator":{"id":714,"name":"Pen Test","role":"test|echo
y3qtahfezd iuchyr96ch||a #' |echo y3qtahfezd iuchyr96ch||a #|\" |echo y3qtahfezd iuchyr96ch||a
#","contact_email":"bianca.napoleonov+coord@cclsolutionsgroup.com","organisation":"CCL","zone_coordinator_lead":
false}}],"state_stage_id":0,"is_pipelined":true,"pipelined_year":"2021"}
```


Response:


```
HTTP/2 200 OK
Date: Thu, 09 Oct 2025 14:14:53 GMT
Content-Type: application/json
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch
"{\"id\":904,\"zone_id\":\"00nw1qpwuXJ-0\",\"fid\":\"906\", --redacted--
```


6.4.3. Recommendations

To address the issue of insufficient input validation, implement robust server-side validation to ensure all input conforms to expected formats, types, and ranges before processing. Define clear validation rules for each input field, such as restricting length, disallowing special characters if unnecessary, or using whitelists for acceptable input patterns. Employ structured validation libraries where available to minimise human error. Additionally, ensure the validation process rejects unexpected or malformed data with informative error messages for the user. Validate all inputs at the point of entry, regardless of the source, including API endpoints and external integrations, to mitigate the risk of injecting unintended or harmful data into the system. By implementing and adhering to these practices, you enhance the reliability and security of your application, reducing vulnerabilities stemming from improperly sanitised input.

6.4.4. References

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

6.4.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.5. Insufficient User Intent Verification for Data Deletion

Severity	Low
Impact	1
Likelihood	1
Fix Effort	Intermediate
Status	Ongoing
Reference	5

6.5.1. Summary

The application allows users to permanently delete data without presenting a confirmation dialog or requiring explicit user intent verification. The design pattern increases the risk of accidental data loss due to misclicks or user error.

6.5.2. Technical Information

It was noted the application allowed users to delete records without a confirmation dialog or a two step process to prevent accidental deletion of critical information.

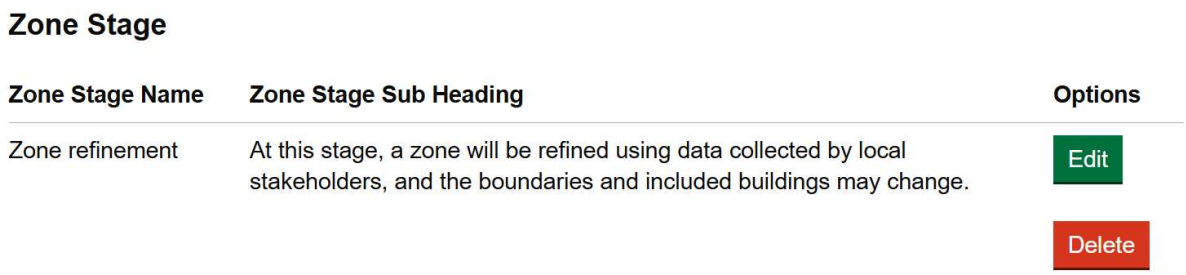


Figure 3 - Delete button does not prompt for confirmation before deleting record.

6.5.3. Recommendations

Implement confirmation dialogs for all destructive actions or consider soft delete with undo functionality.

6.5.4. References

https://owasp.org/Top10/A04_2021-Insecure_Design/

6.5.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.6. SSL Weak Cipher Suites (CBC)

Severity	Low
Impact	2
Likelihood	2
Fix Effort	Intermediate
Status	Ongoing
Reference	6

6.6.1. Summary

SSL certificates are used to encrypt communications and verify identity. To transfer data securely TLS/SSL uses one or more cipher suites, these are used to establish a secure connection. If the connection permits, an attacker could purposely specify to downgrade a connection to use the weakest supported version. Weaknesses in either the protocol or cipher suite, could allow a well-position attacker to Man-in-the-middle (MiTM) traffic, to derive clear-text data from the HTTPS communications which could include cookies, usernames and passwords.

6.6.2. Technical Information

The following cipher suites used Cipher Block Chaining (CBC). These are vulnerable to oracle padding attacks. This attack enables a malicious actor to decrypt the contents of the data, without knowing the key.

Key Exchange	Encryption	Bits	Cipher Suite Name (IANA/RFC)
ECDH 253	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDH 253	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

6.6.3. Recommendations

Weak methods of encryption should be disabled to ensure only secure cipher suites are used. This can be achieved, by removing the outdated ciphers and using secure alternatives. An example of a secure cipher configuration list can be found below.

```
ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
```

6.6.4. References

https://ssl-config.mozilla.org/

https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Transport_Layer_Security_Cheat_Sheet.md

https://learn.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode

6.6.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.7. Excessive Session Timeout Configured

Severity	Low
Impact	1
Likelihood	2
Fix Effort	Intermediate
Status	Ongoing
Reference	7

6.7.1. Summary

Session timeouts determine the amount of time an attacker has to take over an existing session. The lower the session timeout, the less window of opportunity there is for an attacker. The application was found to have an excessive session timeout configured. As a result, user sessions remain active for an unreasonably long period, even when users are inactive. This poses a security risk as it could allow unauthorised users to access sensitive information if they gain access to an abandoned or forgotten session.

Without a proper session timeout policy, an attacker who gains access to a users session (via methods such as session hijacking or cross-site scripting) could potentially perform actions on behalf of the legitimate user or retrieve sensitive data without the users knowledge.

6.7.2. Technical Information

The following screenshot shows the Expire/Max-Age values of the cookies indicating the application was found to have an excessive session timeout configured (close to a month).

Name	Value	Domain	Path	Expires / Max-Age
__Secure-...	eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIn0..yzLlh6fr0xxC3JGY.SPyLFbb-BJWpRhMvpHQLz97ywtoDDT7xt3tgJZ3TUmVSrJBXIwaQzIkurAHLU_8HmiBzhN...	www.heat-n...	/	Wed, 05 Nov 2025 1...
arcgis_to...	1760368305353	www.heat-n...	/	Mon, 13 Oct 2025 1...
arcgis_to...	mzFcMRqhxzPAoRJavp2MJkRRNOon2PShQlI7pGdeXz6ClZ-99WTmts7kMeAjdxYYxOK3kXXoLxl1kjEvwybwa3l0LStVwkPCAy7SuqZGIfFgbwp-d6l11jREofeF...	www.heat-n...	/	Mon, 13 Oct 2025 1...

Figure 4 - Excessive session timeout configured.

6.7.3. Recommendations

Implement a session timeout policy that terminates sessions after a defined period of inactivity. Session timeouts should be set to as minimal a value as possible depending on the context of the application, generally 15 to 30 minutes for administrative accounts and 30 to 60 minutes for low-risk users. Additionally, the application should prompt users with a warning before automatically logging them out, providing them with the option to extend their session. Ensure that session tokens are securely handled and invalidate sessions upon logout to prevent unauthorised reuse.

6.7.4. References

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

6.7.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.8. Concurrent Logins Supported

Severity	Informational
Fix Effort	Intermediate
Status	Ongoing
Reference	8

6.8.1. Summary

The application supports concurrent logins as the same user. Concurrent logins allow the same user to be authenticated in multiple places simultaneously. This provides the user a level of convenience when switching between devices etc. Without concurrent logins it is more likely a user would become aware if their credentials had become known to a malicious threat actor. This is because their session would be terminated when the attacker accessed the application. With multiple concurrent sessions, it becomes more challenging to monitor user activity and maintain a clear audit trail. This can hinder an organisation's ability to detect and investigate suspicious behaviour or security incidents.

6.8.2. Technical Information

It is possible to have multiple active sessions with the application concurrently, as shown in the following screenshot where bianca.napoleonov+user@cclsolutionsgroup.com is logged in on both Edge and Firefox private browsing.

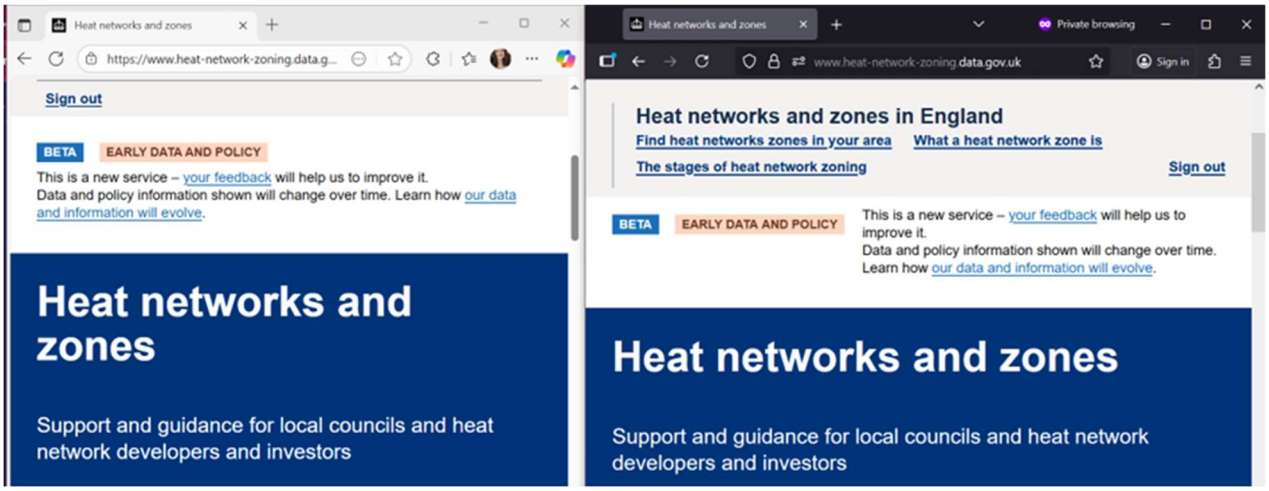


Figure 5 - Concurrent login sessions.

6.8.3. Recommendations

Concurrent logins should be prevented, particularly for privileged accounts. Upon successful authentication, any previous sessions associated with the current user should be invalidated.

6.8.4. References

https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Simultaneous_Session_Logons

6.8.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

6.9. Information Disclosure via HTTP Header

Severity	Informational
Fix Effort	Easy
Status	Ongoing
Reference	9

6.9.1. Summary

Information disclosure can potentially provide a malicious threat actor with additional information that can assist in building an attack picture against the web application and the organisation overall. This is information that is either overly technical or is not useful to normal end users, and it should not be shown. Limit the disclosure of information to developers and administrators within the organisation to assist with troubleshooting.

6.9.2. Technical Information

The application was found to reveal the web framework supporting the service within the HTTP banners. Below is an example response from the /admin part of the application.

Response:

```
HTTP/2 200 OK
Date: Thu, 09 Oct 2025 15:31:42 GMT
Content-Type: text/html; charset=utf-8
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding
X-Nextjs-Cache: HIT
X-Powered-By: Next.js
Cache-Control: s-maxage=31536000, stale-while-revalidate
Etag: "zydbj5dfa9i15"
--redacted--
```

6.9.3. Recommendations

Information about backend services should be redacted. The “X-Powered-By: ” banner should not be returned by the server.

By default Next.js will add the `x-powered-by` header. To opt-out of it, open `next.config.js` and disable the `poweredByHeader` config:

module.exports = { poweredByHeader: false,}

6.9.4. References

https://nextjs.org/docs/app/api-reference/config/next-config-js/poweredByHeader

6.9.5. Affected Systems

Hostname
www.heat-network-zoning.data.gov.uk

Appendix A – Testing Team

Name	Email	Qualifications
Bianca Napoleonov	Bianca.Napoleonov@cclsolutionsgroup.com	CSTL Applications

Appendix B – Reporting Metrics

B.1. Risk Ratings

This section provides information on how risk ratings are calculated within the report.

The following table describes with examples what each level of impact and likelihood represents.

Impact (1-5)	Likelihood (1-5)
1 - This is the lowest level of impact and generally represents information disclosure. For example, a service which discloses software version numbers or other minor information which could aid an attacker in further attacks. However, does not on its own allow a threat actor to launch an attack.	1 - A likelihood of 1 would represent the lowest risk of an issue being exploited. This could be because of the high complexity of the exploit. For example, a vulnerability which would require a highly skilled attacker to exploit. Alternatively, a low likelihood could be due to significant access requirements to leverage the exploit. It could also be a combination of these two things. For example, a vulnerability which can only be exploited from an air-gapped network.
2 - This level of impact refers to; more severe instances of information disclosure, minor configuration weaknesses that could be leveraged by attackers who already have a level of access to systems, or configuration weaknesses which would not directly result in compromise but could reduce the time requirements or difficulty of attacks.	2 - This level of likelihood refers to vulnerabilities that would require a high level of access to exploit, and / or a high level of skill. For example, administrative access may be required to the system, and / or the vulnerability may not be publicly available.
3 - The level of impact refers to vulnerabilities that would give a moderate level of access to systems, or significant information disclosure. For example, gaining access to a system with user-level credentials. Or a system that discloses usernames, emails, or sensitive technical information to unauthenticated attackers.	3 - This level regards vulnerabilities that may require a level of access, either to networks or systems, for an attacker to be suitably positioned to exploit. For example, user-level credentials may be required to perform the exploit. Alternatively, or conjunctively, the vulnerability may require insider knowledge to exploit. At this level of likelihood, the exploit would require a reasonably skilled attacker.
4 - This level of impact represents vulnerabilities that give an attacker a high level of access to systems. For example, gaining administrative level access via privilege escalation to a server, or admin access to an application. Allowing an attacker to affect changes to the system / application.	4 - This level represents vulnerabilities that have a high likelihood of being exploited. For example, a server on an organisations standard corporate network with a vulnerability for which there is publicly available exploit tools.
5 - This is the highest level and would represent an impact which allowed complete compromise of the system. For example, bypassing the login mechanism to access a system as an administrative user. Allowing an attacker to access all data within that system.	5 - This is the highest level of likelihood and refers to vulnerabilities which are trivial to exploit. For example, a vulnerability which is exploitable using automated tools, with very little skill. This could also be due to ease of access. For example, a vulnerability that can be exploited remotely over the Internet using publicly available tools.

The risk rating of an issue is then calculated using the following formula:

Impact + Likelihood = Overall Risk

The table below is used to calculate the severity for that issue:

Overall Risk	Severity
0	Informational
2-4	Low
5-6	Medium
7-10	High

B.2. Fix Effort

The following table describes with examples how the "Fix Effort" is calculated for issues.

Fix Effort	Description
Easy	This represents issues which require minimal effort to remediate. For example, installing security updates, or changing settings.
Intermediate	This represents issues that require a moderate amount of effort to resolve. For example, modifying configuration files, or enabling settings which could cause disruption. For example, settings which provide security, but disable support for legacy clients.
Hard	A fix effort of high relates to vulnerabilities that require the considerable effort to resolve. Potentially requiring work on behalf of the software vendor or in-house web / software development work. This could also relate to issues which require network redesign.

Please note, the fix effort cannot always factor in organisation specific rationale as to the work required to remediate issues. For example, in the case of critical infrastructure. Missing patches may be assigned a "Fix Effort" of Low. However, systems may need to be patched out-of-hours, as they cannot be taken offline during the day. Consequently, the fix effort is calculated solely on the technical complexity of remediating an issue.