Great River Energy Enterprise Security

Jeff Grussing

Why the need?

- You should secure your GIS Enterprise.
- Pros of security measures put in place
  - Make you less vulnerable to attack
  - Protects other systems on the network
  - Ensures users are properly authenticated
- Cons
  - Can limit some functionality

GRE Security Case

- GRE IT was alerted of a security breach involving GIS and another company
  - The GIS vendor was the same as GRE's
  - We wanted to test GRE's GIS to identify any vulnerabilities using our development GIS portal
- GRE engaged a security vendor CLA (CliftonLarsonAllen LLP) to perform the test in October 2023

What is the objective?

RELIABILITY AND SAFETY

- From CLA results report:
  - The objective of the Web Application Penetration Test was to provide valuable insight regarding the ability of Great River Energy's web applications to resist attacks over the internet and locally from unauthorized and valid users

What is the objective?

RELIABILITY AND SAFETY

- Testing was performed in October, 2023
- New user created within GRE system to replicate existing connection configuration
  - GRE domain sample user: u6000
  - CLA had to provide credentials for two-factor authentication process GRE already had in place (PingID)

What did they do?

RELIABILITY AND SAFETY

- Lots and lots of testing
  - Identity management
  - Authentication
  - Authorization
  - Session management
  - Input validation
  - Error handling
  - Cryptography
  - Business logic
  - Client side

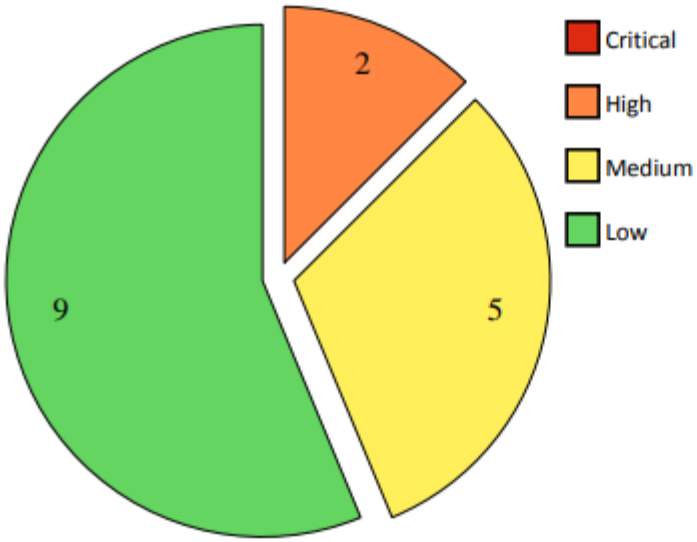
Results

RELIABILITY AND SAFETY

- For the most part, GRE was secure

Finding Severity Chart (Unique Findings)

The pie chart below represents the number of unique findings for each severity level.



Results

RELIABILITY AND SAFETY

Summary of Findings

The table below summarizes the observations from the engagement. For technical details and remediation strategies for each of these findings, please see the accompanying spreadsheet.

Table 3: Summary of Findings

Finding	Description	Severity
1	Multi-factor authentication (MFA) not required	High
2	Unauthenticated Access to Web Application Proxy	High
3	Cross-site request forgery	Medium
4	Session token in URL	Medium
5	Strict transport security not enforced	Medium
6	Web application administration page exposed to internet.	Medium
7	F5 BIG-IP Cookie Remote Information Disclosure	Medium
8	Ajax request header manipulation (DOM-based)	Low
9	Cacheable HTTPS response	Low
10	Cookie without HttpOnly flag set	Low
11	Cross-origin resource sharing: arbitrary origin trusted	Low
12	Missing or Permissive Content-Security-Policy HTTP Response Header	Low
13	Missing or Permissive X-Frame-Options HTTP Response Header	Low
14	Open redirection (DOM-based)	Low
15	TLS cookie without secure flag set	Low
16	Vulnerable JavaScript dependency	Low

Results – first high-risk vulnerability

RELIABILITY AND SAFETY

- First high-risk vulnerability
  - [High] Authentication to the application, from users outside GRE's internal network, relies on push notifications through a third-party application. Attackers can abuse this to trick employees into accepting rogue authentication prompts and gain access to the web application
  - An attacker, with a list of usernames, may be able to trick a user into accepting a rouge authentication prompt and gain access to system

Results – first high-risk vulnerability, cont'd

RELIABILITY AND SAFETY

- Solution:
  - User education
    - Never approve PingID authentication prompt unless you are actively logging into GIS system
    - Applies to GRE employees and approved contractors with access to GIS system (construction, vegetation, etc.)
  - CLA recommended multi-factor authentication (MFA) to the application
    - GRE already has two-factor authentication in place, no intention of moving to MFA

Results – second high-risk vulnerability

RELIABILITY AND SAFETY

- Second high-risk vulnerability
  - [High] The web application allowed unauthenticated use of a feature that allowed CLA to enumerate open ports on the load balancing server and other endpoints across GRE's internal network
  - An attacker may be able to enumerate the server or internal network to obtain information about open ports or other services running on network

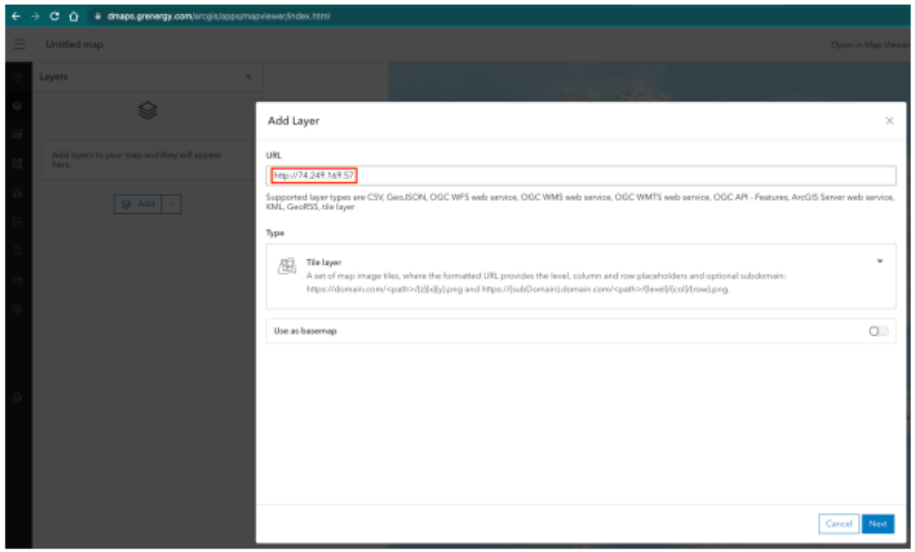
Results – second high-risk vulnerability, cont'd

RELIABILITY AND SAFETY

- CLA was able to launch an empty web map and inset a URL into the 'Add Layer' tool in the web map. From there they were able to modify the proxy request to enumerate the GRE internal network and gain access to other business systems on the network like the Cisco phone system

Results – second high-risk vulnerability, cont'd

RELIABILITY AND SAFETY



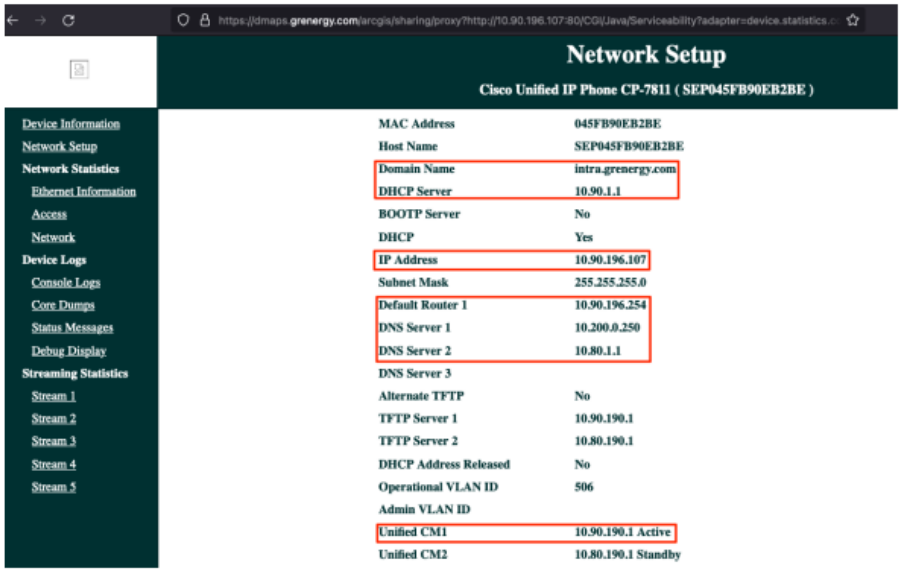


Image 5: Accessing the web page for an internal Cisco phone to obtain additional network information.

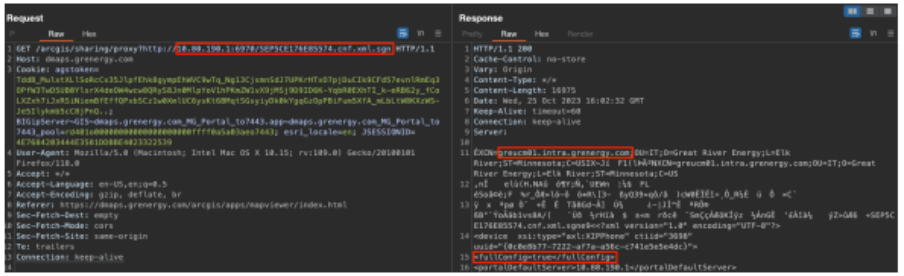
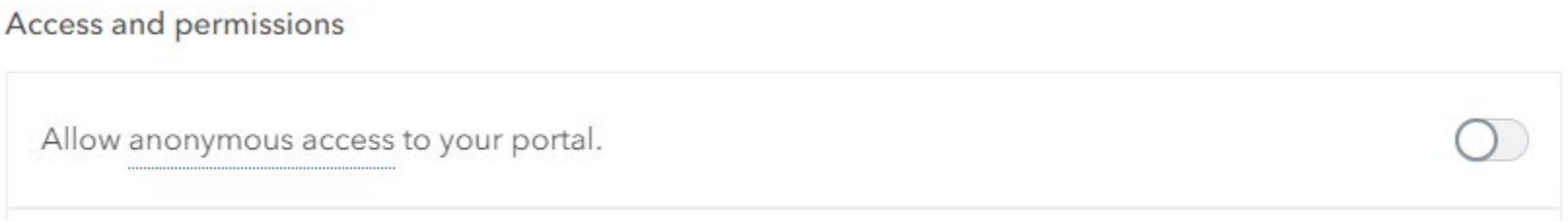


Image 6: Requesting Cisco phone configuration files from the Cisco Unified Communications Manager server.

Results – second high-risk vulnerability, cont'd

RELIABILITY AND SAFETY

- Solution:
  - Restrict anonymous access to portal
    - Dev GIS portal had this feature unintentionally turned on, now it is turned off



Results – second high-risk vulnerability, cont'd

RELIABILITY AND SAFETY

- Solution:
  - Disable access to rest end point of GIS servers (mapping and data store) to restrict access to end point of GIS services w/o proper credentials
  - Restrict proxy access to just the servers part of GIS portal

Services Directory :	Disabled.
Callback Functions Enabled :	Enabled.
AllowedOrigins :	https://dcbdevgis01.intra.grenergy.com, https://dcbdevgis02.intra.grenergy.com, https://dmgdevgis01.intra.grenergy.com, https://dmgdevgis02.intra.grenergy.com, https://dcbdevport01.intra.grenergy.com, https://dcbdevport02.intra.grenergy.com, https://dmgdevport01.intra.grenergy.com, https://dmgdevport02.intra.grenergy.com, https://dcbdevrds01.intra.grenergy.com, https://dcbdevrds02.intra.grenergy.com, https://dmgdevrds01.intra.grenergy.com, https://dmgdevrds02.intra.grenergy.com, https://dcbdevgeo.intra.grenergy.com, https://dmgdevgeo.intra.grenergy.com, https://mgprodpro01.intra.grenergy.com, https://mgprodpro02.intra.grenergy.com

- Other Esri best security practices
  - Closing of the rest end point
  - Proxy urls
  - Disabling ArcGIS Server Admin
    - ArcGIS Monitor connection issue – can’t monitor when admin disabled

Conclusion

RELIABILITY AND SAFETY

- GIS worked with IT to ensure all high, medium, and low risks issues were addressed
- Actions taken on development GIS portal were also completed in production GIS portal
- It was a beneficial and helpful exercise that provided good education to GIS about cyber security and best practices to prevent an attack