

ArcGIS Enterprise – Security Best Practice

Gerhard “Luigi” Trichtl

Esri User Conference Austria 2025 – powered by SynerGIS

Security Media-Hype

- zB. Letzte Woche Chinese Hackers Exploit ArcGIS Server as Backdoor for Over a Year

Flax Typhoon is known for living up to the "stealth" in its tradecraft by extensively incorporating living off the land (LotL) methods and hands-on keyboard activity, thereby turning software components into malicious attacks, while simultaneously evading detection.

The attack demonstrates how attackers increasingly abuse trusted tools and services to bypass your organization. Based on our findings, this issue appears in default configurations and is widespread, with hundreds of hosts vulnerable worldwide.

We have reported this to the vendor, who informed us they consider it a configuration issue and will not be taking further action. As such, we are proactively reaching out to organizations hosting a vulnerable instance to help mitigate potential risks.

To ensure this information reaches the appropriate security team, could you please direct this message to the correct contact person or department responsible for vulnerability management?

We are happy to provide all the necessary technical details to assist with remediation.

The "unusually clever attack chain" involved the threat actors targeting a public-facing ArcGIS server by compromising a portal administrator account to deploy a malicious SOE.

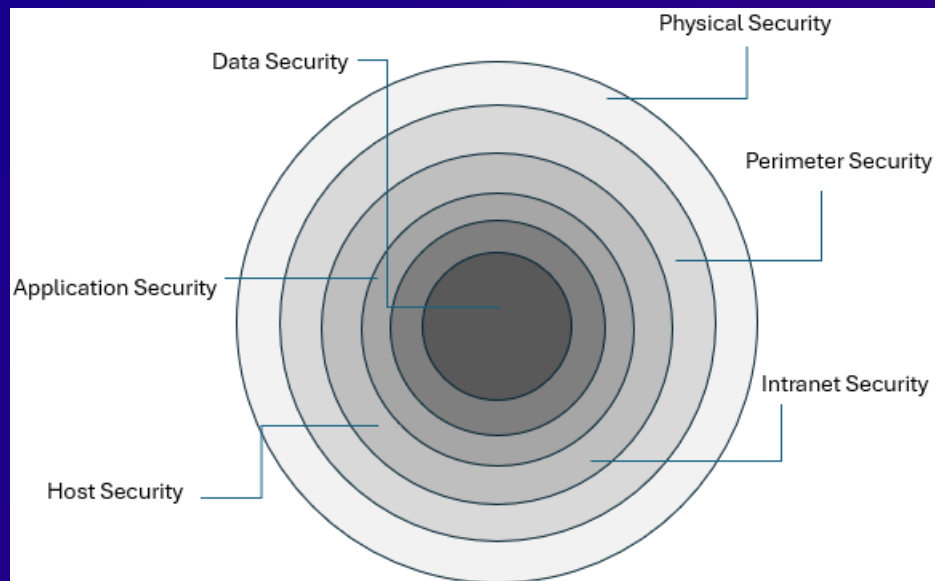
"The attackers activated the malicious SOE using a standard [JavaSimpleRESTSOE] ArcGIS extension, invoking a REST operation on the internal server via the public portal—making their activity difficult to spot," ReliaQuest said. "By adding a hard-coded key, Flax Typhoon prevented other attackers, or even curious admins, from tampering with its access."



Defense In Depth Paradigm

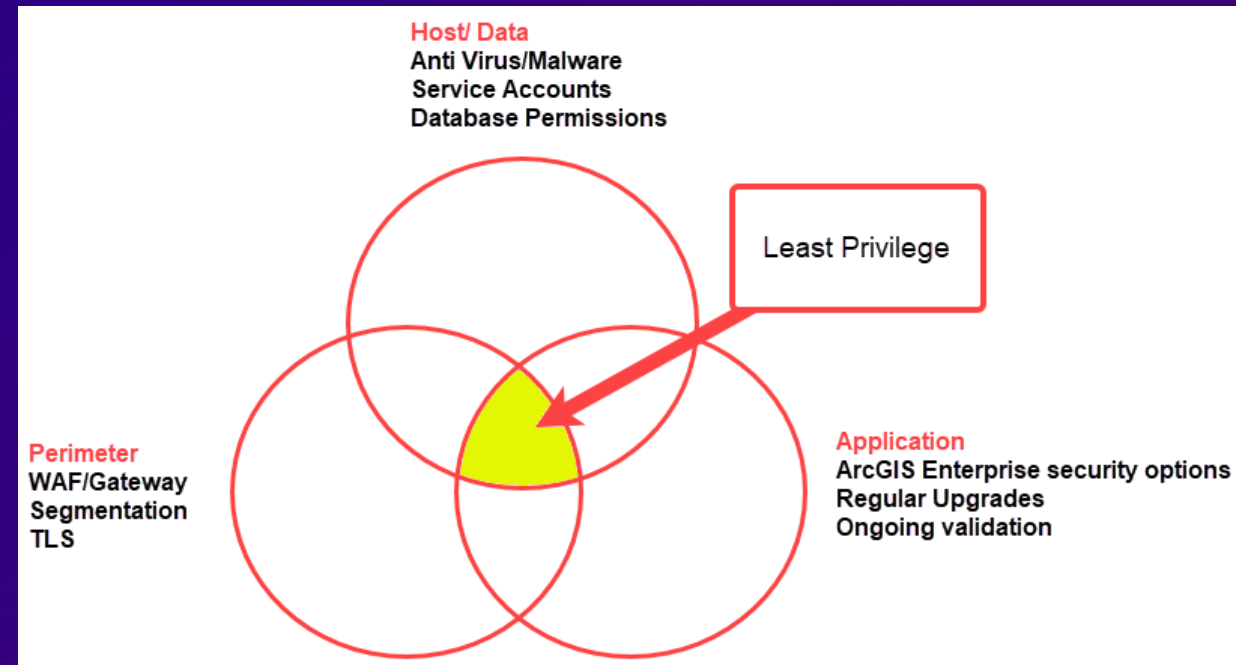
Esri provides tools, but can't compensate for tools beyond the application tier

- Security plans have many “**layers**” – **multiple levels of security**
- Layered security mechanisms increase the security of the system as a whole
- Each feature discussed is considered a “layer”
- WAF, SIEM, Anti-Virus, Encryption, SAML/OIDC identity stores, application config, etc



Fundamentals

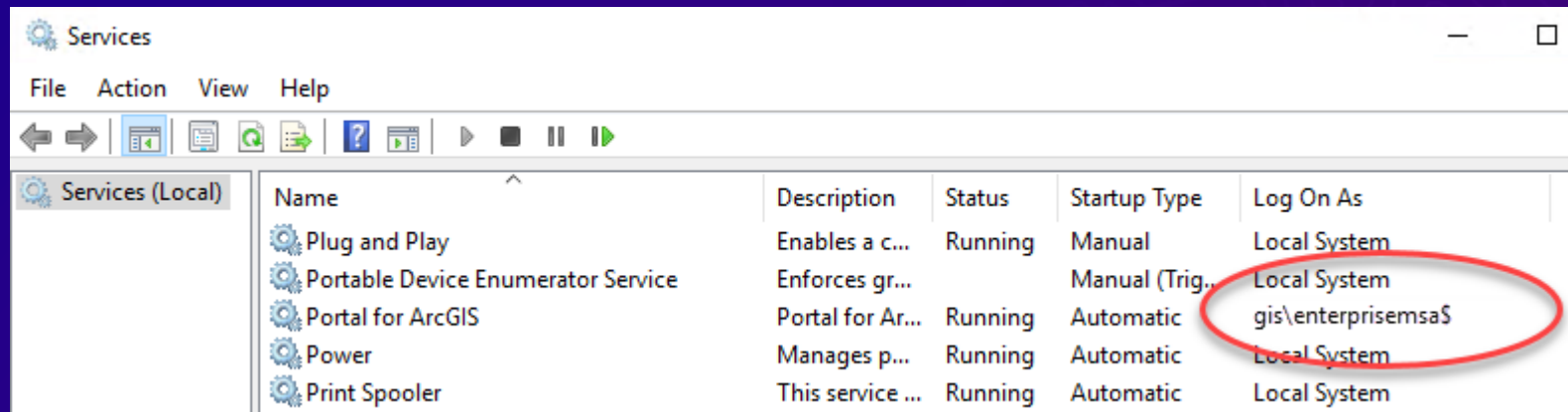
- Principle of LEAST privilege
 - **NOT Principle of MOST privilege**
 - Limit admin accounts.
 - Use custom roles
 - Limit Service account permissions
 - Use gMSA (Group Managed Service Accounts)
 - Upgrades are important
 - Updated components/features
- Segmentation
 - Cloud first!



What's a gMSA?

Windows only

- Restricted Active Directory domain account
- Can only be used in a few places on Windows
 - “Log On As” account for Windows Services
 - IIS application pool identity
 - User account to run scheduled tasks
- “\$” is appended to the end of the account to indicate it is a gMSA



The screenshot shows the Windows Services console window. The 'Log On As' column for the 'Portal for ArcGIS' service is circled in red, showing the account 'gis\enterprisemsa\$'.

Name	Description	Status	Startup Type	Log On As
Plug and Play	Enables a c...	Running	Manual	Local System
Portable Device Enumerator Service	Enforces gr...		Manual (Trig...	Local System
Portal for ArcGIS	Portal for Ar...	Running	Automatic	gis\enterprisemsa\$
Power	Manages p...	Running	Automatic	Local System
Print Spooler	This service ...	Running	Automatic	Local System

gMSA: Security benefits

- Password is managed internally by Active Directory
- Does not have a static password
 - Password is 128 UTF-16 characters
 - Automatically changed every 30 days (by default)
- No interactive logins
- Restricted to a pre-defined set of computers

Upgrades are important

Patches are also important





Yes, upgrades can be painful

But...

- Updates to 3rd party components with each release
 - Reduce noise from security scans
- Access to new functionality
 - New logging functionality in 11.4/11.5
 - New Content Security Policy support at 11.4/11.5
- Automate patchNotification
 - PatchNotification can be scheduled
 - CRON job or Windows Scheduled task

```
:: Typical usage:
:: > patchnotification.bat -c          # Show patch information
:: > patchnotification.bat -c -i sec  # Install security patches only for
::                                     # installed products
:: > patchnotification.bat -c -i all  # Install all available patches for
::                                     # installed products
```

```
C:\Program Files\ArcGIS\Portal\tools\patchnotification>patchnotification.bat -c
=====
                        ArcGIS Enterprise Patch Notification
=====

Installierte Komponenten

ArcGIS Data Store          11.5
ArcGIS Server              11.5
Portal for ArcGIS         11.5
=====

Verfügbare Aktualisierungen

ArcGIS Data Store
(keine Aktualisierungen verfügbar)

ArcGIS Server
- ArcGIS Server Feature Services Security Patch (!)
  https://support.esri.com/en-us/patches-updates/2025/arcgis-server-feature-services-security-patch
  Veröffentlichungsdatum: 07.10.25

Portal for ArcGIS
- Portal for ArcGIS Mission Manager Location Services and Projection Patch
  https://support.esri.com/en-us/patches-updates/2025/portal-for-arcgis-mission-manager-location-services-and-proje
tion-patch
  Veröffentlichungsdatum: 06.10.25
=====

Installierte Patches
- Portal for ArcGIS 11.5 Mission Manager Location Services and Projection Patch
- Portal for ArcGIS 11.5 Web Applications Patch
- ArcGIS Server 11.5 Branch Versioning Licensing Patch
- ArcGIS Server 11.5 Calculate Field Patch
- ArcGIS Server 11.5 Utility Network Patch 1
- ArcGIS Server 11.5 ArcGIS Pipeline Referencing/ArcGIS Roads and Highways Patch 1
=====

Um eine vollständige Liste der Patches und Service Packs von Esri zu durchsuchen, besuchen Sie die Support-Website von E
sri:
http://support.esri.com/Downloads
```

Security options



Restrict Proxy Capability

...**STRONGLY RECOMMENDED MUST DO**

The portal's proxy:
Unrestricted by default

Portal Administrator Directory

Home > Security > Config > Update Security Configuration

Update Security Configuration

Configuration (in JSON format) *

```
{ "disableServicesDirectory": false, "enableAutomaticAccountCreation": false, "contentSecurityPolicy": { "home": "frame-ancestors 'self';", "apps": "", "sharing": "script-src 'self';" }, "webgisServerTrustKey": "fEJJHN3wdA2ZNd3NY2WcgmE5iG2nZsiQM5qZcSTWRvo=", "disableServicesDirectory": true, "allowedProxyHosts": "gisserver1.domain.com,gisserver2.domain.com" }
```

Format

- Supports saving credentials for secured servers accessed remotely
- Needed for viewing KML and GeoRSS endpoints
- Define hosts to where Portal can proxy
 - PREVENT Denial of Service (DOS)
 - PREVENT Server-Side Request Forgery (SSRF)

Zulässige Proxy-Hosts

Konfigurieren Sie eine Liste von Hostnamen oder Domänen, auf die die Proxy-Funktion des Enterprise-Portals zugreifen darf. Platzhalter werden im Format "(.*)example.com" unterstützt, um den Zugriff auf alle Computer innerhalb einer bestimmten Domäne zuzulassen.

(.*).arcgis.com	<input type="text" value="x"/>
(.*).arcgisonline.com	<input type="text" value="x"/>
gisupdates.esri.com	<input type="text" value="x"/>
lws-job-results-prd0-apse2.s3.amazonaws.com	<input type="text" value="x"/>
lws-job-results-prd0-euw1.s3.amazonaws.com	<input type="text" value="x"/>
lws-job-results-prd0-use1.s3.amazonaws.com	<input type="text" value="x"/>

portalScan.py

enterprise.arcgis.com > Search "portalScan.py"

Portal for ArcGIS Security Scan Report - 06/30/25

uc2025.esri.com (11.5)

Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
PS01	Critical	Proxy restrictions	The portal proxy capability is unrestricted. This should be limited to trusted web addresses. More information Suggested "allowedProxyHosts" based on existing maps, services, and configuration settings: droughtmonitor.unl.edu, earthquake.usgs.gov, sampleserver6.arcgisonline.com
PS14	Important	Default print service status	The default print service distributed with your portal is currently enabled. Since the portal is already configured to use a print service from ArcGIS Server, it is recommended to disable the default print service. More information
PS03	Important	Portal services directory	The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information
PS06	Recommended	Anonymous access	To prevent any user from accessing the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information
PS09	Recommended	Cross-domain requests	Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information
PS17	Recommended	KML service status	The KML service is used by the portal to communicate with KML endpoints. If no KML endpoints will be accessed through any web maps on the portal, it is recommended to disable this service. More information
PS16	Recommended	RSS service status	The RSS service is used by the portal to communicate with GeoRSS feeds. If no GeoRSS feeds will be accessed through any web maps on the portal, it is recommended to disable this service. More information

Use SAML or OpenID Connect

AKA: Organization Specific Logins

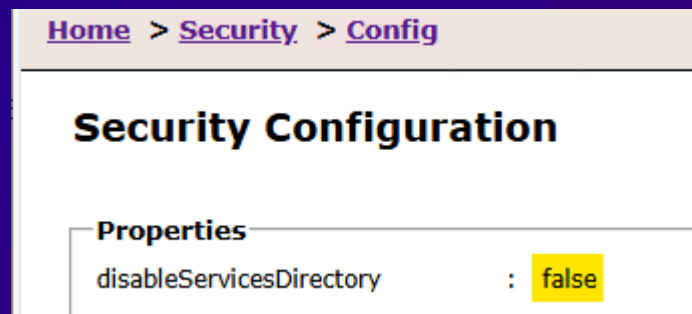
- Centralized user repository – use your existing identity provider
- Automatically integrates with MFA
 - MFA for ArcGIS accounts also available
 - Requires email server integration
 - Requires two Admin Accounts
- Industry standard
- Can be configured to auto-assign ArcGIS Enterprise Group Membership
- Configuration Details:
 - [Configure a SAML-compliant identity provider with a portal—Portal for ArcGIS | Documentation for ArcGIS Enterprise](#)
 - [Configure OpenID Connect logins—Portal for ArcGIS | Documentation for ArcGIS Enterprise](#)

Disable Services Directories

Reduces Potential Attack Surface

- Prevents service listing by bots / search engines
- Does NOT limit functionality – just hides HTML form driven view
- Recommend to not expose:
 - ArcGIS Portal Directory
 - ArcGIS Server REST Services Directory
- Use Case Dependent Option

Portal for ArcGIS



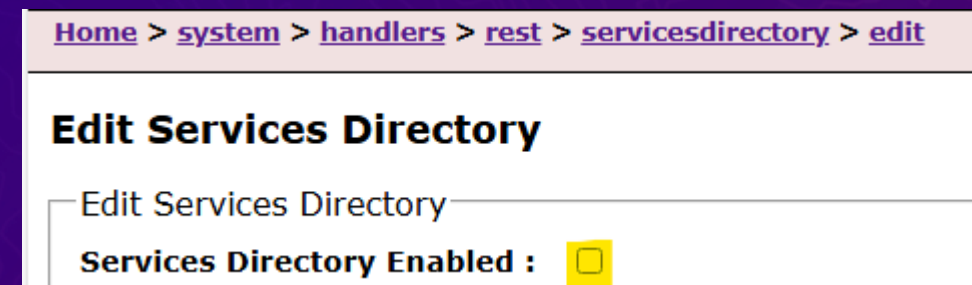
Home > Security > Config

Security Configuration

Properties

disableServicesDirectory	:	false
--------------------------	---	-------

ArcGIS Server



Home > system > handlers > rest > servicesdirectory > edit

Edit Services Directory

Edit Services Directory

Services Directory Enabled :

New Capability: Content Security Policy

If you choose to expose the services directory...

- CSP allows another level of protection against cross-site-scripting (XSS)
- Consistent with defense in depth approach
- The default CSP will block potential XSS attacks against
 - ArcGIS Portal Directory
 - ArcGIS Server REST Services Directory

- Configuration Details:
 - [Configuration \(Security\) | ArcGIS REST APIs | Esri Developer](#)

Use Hosted Feature Service Views

What is a view?

- Allows publishers to control which data a user sees.
- View definition:
 - Spatial Extent
 - Define visible fields
 - NOT the same as an attribute filter

Why use a view?

- Hide Sensitive information from authorized users
- Show non-sensitive information to wider audience
- Create apps for different audiences
- All referencing same data source

Field Visibility

- Does choosing specific fields to show in a popup meaningfully improve **SECURITY**?
- NO.**
- Choosing fields displayed in a popup does NOT change what fields can be queried
- Using a VIEW LAYER is the solution**

Example: View Architecture

ArcGIS Online Data Editing and Management



Parent Hosted
Feature Layer



Public Submitters View

- Query disabled
- Add only
- Shared with public



Mobile Offline View

- Add only
- Enable sync
- Webmap offline areas
- Shared with mobile group



Approval View

- Query enabled
- Update only
- Shared with QA group



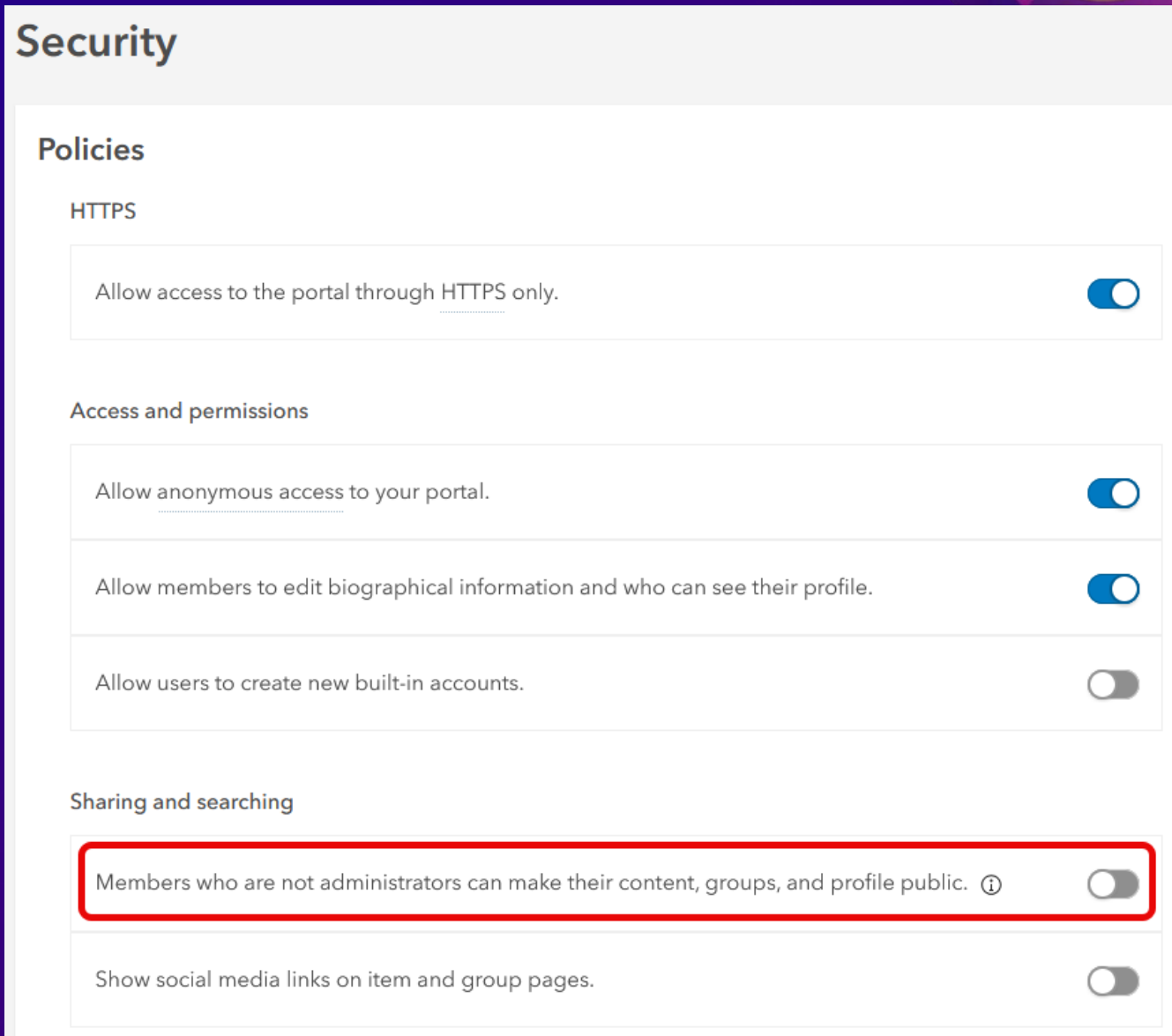
View Only View

- Configured with current user keyword - **New!**
- Filtered by Status and logged in user
- View only
- Shared with org



Restrict public sharing

- Limits who can share with “Everyone”
 - Administrators can set
 - Does not change sharing level on existing items
 - Admins can ALWAYS share publicly
 - Suggestion: Set content review policy to prevent unintended sharing, allow admin to share public.



Security

Policies

HTTPS

Allow access to the portal through [HTTPS](#) only.

Access and permissions

Allow [anonymous access](#) to your portal.

Allow members to edit biographical information and who can see their profile.

Allow users to create new built-in accounts.

Sharing and searching

Members who are not administrators can make their content, groups, and profile public. ⓘ

Show social media links on item and group pages.

portalScan.py

enterprise.arcgis.com > Search "portalScan.py"

Portal for ArcGIS Security Scan Report - 06/30/25

uc2025.esri.com (11.5)

Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>									
PS01	Critical	Proxy restrictions	The portal proxy capability is unrestricted. This should be limited to trusted web addresses. More information Suggested "allowedProxyHosts" based on existing maps, services, and configuration settings: droughtmonitor.unl.edu, earthquake.usgs.gov, sampleserver6.arcgisonline.com									
PS14	Important	Default print service status	The default print service distributed with your portal is currently enabled. Since the portal is already configured to use a print service from ArcGIS Server, it is recommended to disable the default print service. More information									
PS03	Important	Portal services directory	The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information									
PS06	Recommended	Anonymous access	To prevent any user from accessing the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information									
PS09	Recommended	Cross-domain requests	Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information									
PS17	Recommended	KML service status	The KML service is used by the portal to communicate with KML endpoints. If no KML endpoints will be accessed through any web maps on the portal, it is recommended to disable this service. More information									
PS12	Recommended	Public content	The portal is configured so members cannot share content publicly but the following items are currently shared with everyone and may need to be updated. <table><thead><tr><th>Item Name</th><th>Item Type</th><th>Owner</th></tr></thead><tbody><tr><td>California</td><td>Feature Service</td><td>admin</td></tr><tr><td>California Map</td><td>Web Map</td><td>admin</td></tr></tbody></table>	Item Name	Item Type	Owner	California	Feature Service	admin	California Map	Web Map	admin
Item Name	Item Type	Owner										
California	Feature Service	admin										
California Map	Web Map	admin										
PS16	Recommended	RSS service status	The RSS service is used by the portal to communicate with GeoRSS feeds. If no GeoRSS feeds will be accessed through any web maps on the portal, it is recommended to disable this service. More information									

Feature Layer Security and Editing

- Users who can always edit
 - Owner
 - Admins
 - Members of Groups w/ Update capability
- Enable Editing: Defaults
 - Anyone who can access the service can edit
 - Add, update and delete features
 - Only update feature attributes
 - See and edit all features

Data Source Cancel Save

Editing

Enable editing

Keep track of changes to the data (add, update, delete features).

Keep track of who edited the data (editor name, date and time).

Enable Sync (required for offline use and collaboration).

• Who can edit features?
Share the layer to specific groups of people, the organization or publicly via the Share button on the Overview tab. This layer is not shared.

• What kind of editing is allowed?

Add

Delete

Update

Attributes only

Attributes and geometry

• What features can editors see?

Editors can see all features

Editors can only see their own features (requires editor tracking)

Editors can't see any features, even those they add

• What features can editors edit?

Editors can edit all features

Editors can only edit their own features (requires editor tracking)

• Who can manage edits?

- You
- Administrators
- Data curators with the appropriate privileges

Feature Layer Security and Editing

- Considerations for Sensitive Content

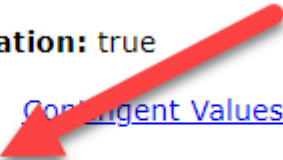
- Disable delete and update
- Enable “Editors can’t see features, even those they add”
- This disables “Query” capability on the service
- If users can query features, they can see data

Supports Query with Historic Moment: false

Supports Coordinates Quantization: true

Child Resources: [Field Groups](#) [Contingent Values](#)

Supported Operations: [Query](#) [Query Attachments](#) [Query Analy](#)
[Metadata](#) [Update Metadata](#)



Data Source

Editing

- Enable editing
- Keep track of changes to the data (add, update, delete features).
- Keep track of who edited the data (editor name, date and time).
- Enable Sync (required for offline use and collaboration).

• Who can edit features?
Share the layer to specific groups of people, the organization or publicly via the Share

• What kind of editing is allowed?

- Add
- Delete
- Update

• What features can editors see?

- Editors can see all features
- Editors can only see their own features (requires editor tracking)
- Editors can't see any features, even those they add

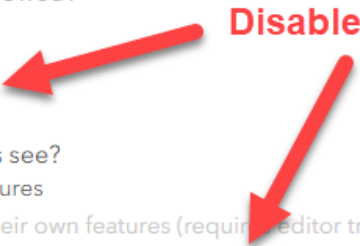
• What features can editors edit?

- Editors can edit all features
- Editors can only edit their own features (requires editor tracking)

• Who can manage edits?

- You
- Administrators
- Data curators with the appropriate privileges

Disables "query"



serverScan.py

enterprise.arcgis.com > Search “serverScan.py”

ArcGIS Server Security Scan Report - 06/30/25

uc2025.esri.com (11.5)

Potential security items to review

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
SS08	Important	Cross-domain requests	Cross-domain requests for REST endpoints are unrestricted. To reduce the possibility of an unknown application sending malicious requests to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. More information
SS08	Important	Cross-domain requests	Cross-domain requests for SOAP endpoints are unrestricted; this applies to OGC endpoints (WMS, WFS, etc.) that are exposed as well. To reduce the possibility of an unknown application sending malicious requests to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. More information
SS07	Important	Rest services directory	The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. More information
SS12	Recommended	Feature service operations	Feature service: Hosted/Airports This feature service has the update and/or delete operations enabled and is open to anonymous access. This allows the feature service data to be changed and/or deleted without authentication.
SS11	Recommended	PSA account status	The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your configuration. More information

More Tools and Docs

- Tools

- Aggregate and examine ArcGIS Enterprise logs with 3rd party tools
- Security and Privacy Advisor, portalScan.py, serverScan.py
 - Identify potential problems early
 - Prevent configuration drift
- Some checks also in the operationalHealthCheck

- DOCS

- ArcGIS Enterprise security best practices documentation
- ArcGIS Enterprise Hardening Guide
- ArcGIS Trust Center

Low Hanging Fruit...

Security Scans will flag...

TLS issues

CORS issues

Outdated Components

Information disclosure via HTTP headers

“Unprotected APIs”

HSTS issues

Content Security Policy issues

On and on and on...

Proactively Identify!



© 2025 Adobe Stock. All rights reserved.



AN ESRI
TECHNICAL PAPER
July 2025

ArcGIS Enterprise Hardening Guide

Table 4-Postinstallation **Basic** Security Controls

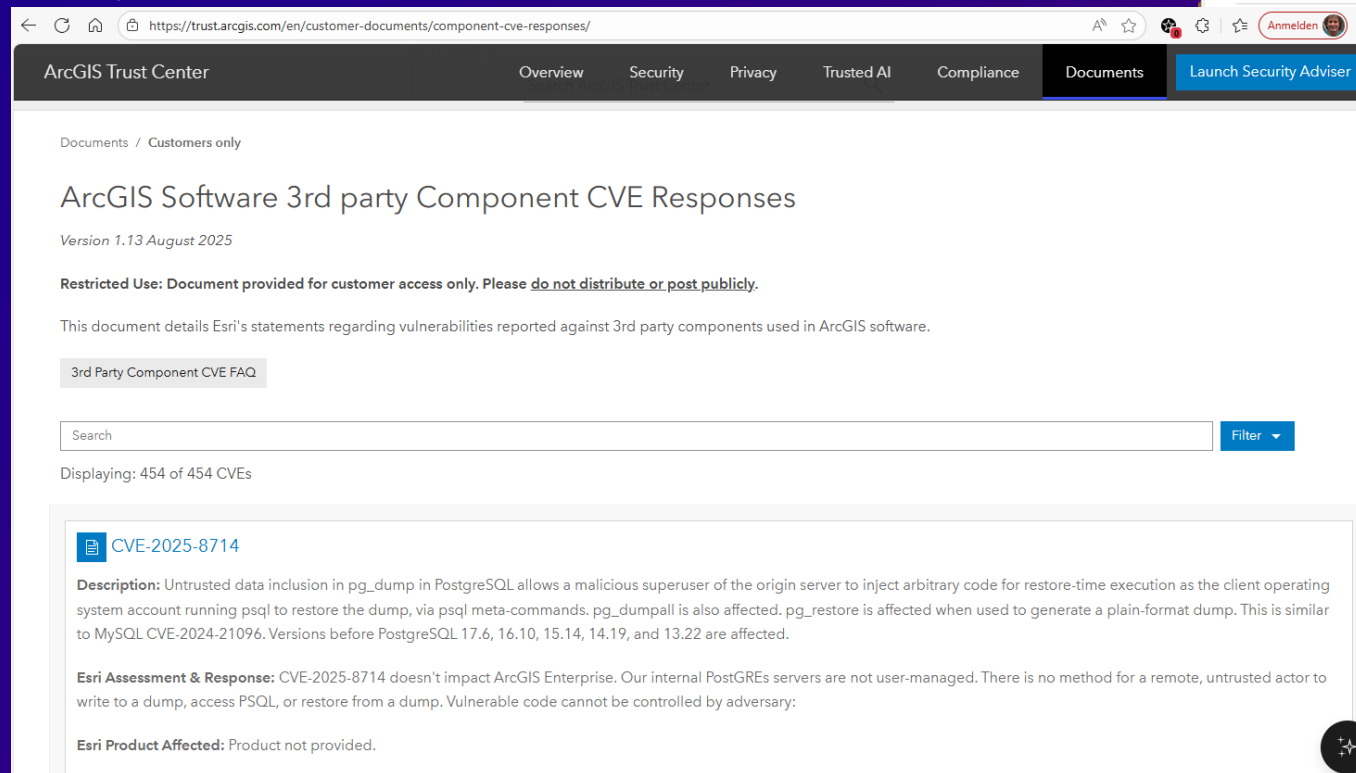
#	Control	Responsible	Prerequisites
1	Basic: Remove Silverlight and FLEX Policy Files	SA	Pre 10.8.1
2	Basic: Consider Disabling Anonymous Access	GA	-
3	Basic: Verify Self-Creation Built-In User Accounts Disabled	GA	-
4	Basic: Verify Dynamic Workspaces/Layers Map Services Disabled	GA	-
5	Basic: Verify Token Acquisition via HTTP GET Disabled	GA	-
6	Basic: Verify Portal for ArcGIS Legend Servlet Disabled	GA	-
7	Basic: Verify Portal for ArcGIS Print Servlet Disabled	GA	-
8	Basic: Verify Portal for ArcGIS WFS Servlet Disabled	GA	-
9	Basic: Configure Access Notice / Information Banners	SA	-
10	Basic: Configure Built-In Accounts Password Policy	GA	Built-In Accounts
11	Basic: Verify Standardized Queries Enabled	GA	-
12	Basic: Verify Header Enabled	GA	-
13	Basic: Configure ArcGIS Logging Level	GA	-
14	Basic: Implement Centralized User Account Management	SA, GA	-
15	Basic: Disable Members Can Share Content Publicly	GA	-
16	Basic: Disable Public User Profile Sharing for Organization Users	GA	-
17	Basic: Implement SAML Signed and Encrypted Assertions	SA, GA	SAML IDP
18	Basic: Configure New Member Default Role as Viewer	GA	-
19	Basic: Implement Password Reset Email Notification	SA, GA	SMTP Server
20	Basic: Implement Signed CA Certificates	SA, GA	Obtain CA Cert
21	Basic: Configure Portal for ArcGIS Proxy Allow List	SA, GA	-
22	Basic: Disable Primary Site Administrator Account (ArcGIS Server)	GA	New PAA
23	Basic: Disable ArcGIS Server Services Directory	GA	-
24	Basic: Disable ArcGIS Portal Directory	GA	-

Security Media-Hype

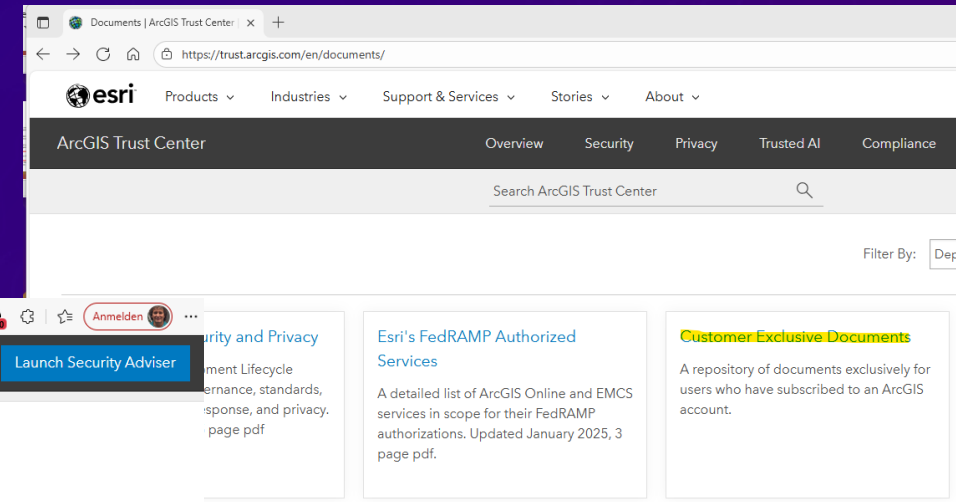
- E.g. [Chinese Hackers Exploit ArcGIS Server as Backdoor for Over a Year](#)
- Easy to say – Hard to verify
- <https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/understanding-arcgis-server-soe-compromise>
- Bei Fragen uns kontaktieren

3rd Party CVE-Responses

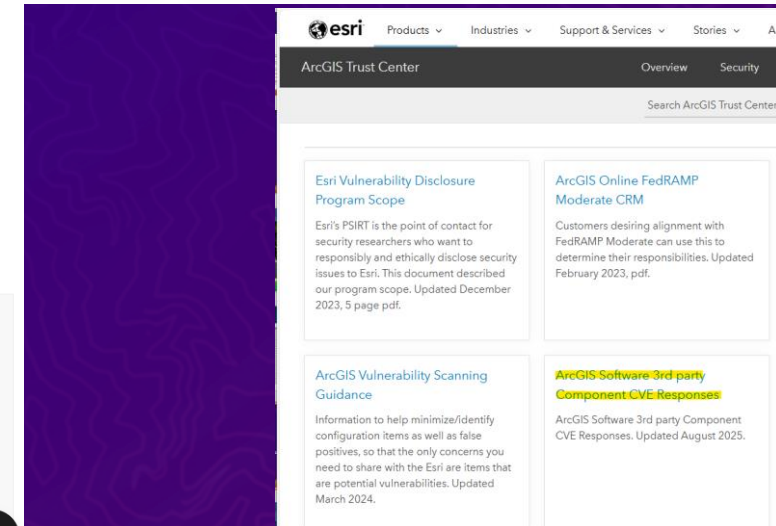
- ArcGIS verwendet viele 3rd Party Komponenten
- Nicht alle Common Vulnerabilities and Exposures (CVE) einer 3rd Party betreffen direkt ArcGIS



The screenshot shows the ArcGIS Trust Center page for '3rd Party Component CVE Responses'. The page title is 'ArcGIS Software 3rd party Component CVE Responses' with a version of '1.13 August 2025'. A warning states: 'Restricted Use: Document provided for customer access only. Please do not distribute or post publicly.' The page includes a search bar and a filter dropdown. The first entry is for CVE-2025-8714, with a description: 'Untrusted data inclusion in pg_dump in PostgreSQL allows a malicious superuser of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql meta-commands. pg_dumpall is also affected. pg_restore is affected when used to generate a plain-format dump. This is similar to MySQL CVE-2024-21096. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected.' The 'Esri Assessment & Response' section states that this CVE does not impact ArcGIS Enterprise. The 'Esri Product Affected' section indicates 'Product not provided.'



The screenshot shows the ArcGIS Trust Center homepage. The navigation menu includes 'Products', 'Industries', 'Support & Services', 'Stories', and 'About'. The main navigation bar includes 'ArcGIS Trust Center', 'Overview', 'Security', 'Privacy', 'Trusted AI', and 'Compliance'. A search bar is located below the navigation bar. On the right side, there are three featured documents: 'Security and Privacy', 'Esri's FedRAMP Authorized Services', and 'Customer Exclusive Documents'.



The screenshot shows the ArcGIS Trust Center 'Security' page. The navigation menu includes 'Products', 'Industries', 'Support & Services', 'Stories', and 'About'. The main navigation bar includes 'ArcGIS Trust Center', 'Overview', and 'Security'. A search bar is located below the navigation bar. On the right side, there are four featured documents: 'Esri Vulnerability Disclosure Program Scope', 'ArcGIS Online FedRAMP Moderate CRM', 'ArcGIS Vulnerability Scanning Guidance', and 'ArcGIS Software 3rd party Component CVE Responses'.

Fragen?





synergis   **esri**™ Official
Distributor

Copyright © 2025 Esri. All rights reserved.