مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Targeted Attacks Against ArcGIS Enterprise Account Recovery Mechanism

Tracking #:432319172

Date:22-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Esri has issued a security advisory warning that threat actors are actively targeting ArcGIS Enterprise deployments by exploiting weaknesses in the built-in account recovery (Forgot Password) workflow.

TECHNICAL DETAILS:

Esri has issued a security advisory warning that threat actors are actively targeting ArcGIS Enterprise deployments by exploiting weaknesses in the built-in account recovery (Forgot Password) workflow. Rather than attacking primary authentication mechanisms protected by Multi-Factor Authentication (MFA), attackers are leveraging insecure account recovery configurations to gain unauthorized administrative access.

Organizations using built-in ArcGIS Enterprise accounts are at immediate risk if recommended security hardening measures have not been implemented. While no software vulnerability (CVE) has been assigned, the issue represents an actively exploited security weakness in account recovery configurations. Esri has confirmed that a security patch is under development and recommends organizations immediately implement the published mitigation guidance.

Technical Details

Esri has observed attackers shifting their focus from primary authentication mechanisms to remote password recovery workflows after many organizations strengthened authentication using Multi-Factor Authentication (MFA).

The attack targets environments that rely on built-in ArcGIS Enterprise accounts instead of centralized identity providers.

A typical attack involves:

- Identifying exposed ArcGIS Enterprise deployments.
- Enumerating existing built-in user accounts.
- Exploiting weak account recovery questions.
- Leveraging predictable administrator usernames.
- Performing unauthorized password reset requests.
- Obtaining full control of compromised built-in accounts.

Successful exploitation may allow attackers to:

- Gain unauthorized administrative access.
- Reset privileged account passwords.
- Access sensitive GIS datasets.
- Modify or delete geospatial information.
- Establish persistent access within the ArcGIS environment.
- Potentially pivot into connected enterprise systems.

Affected Configurations

The advisory affects:

- ArcGIS Enterprise deployments utilizing built-in application accounts.
- Environments with Portal PSA accounts enabled.
- Environments with Server IAA accounts enabled.
- Deployments using weak password recovery questions.
- Deployments using common administrator usernames.
- Systems without SMTP-enabled account validation.

Not affected:

- Organizations exclusively using centralized identity providers (Active Directory, Azure AD, SAML, LDAP, etc.) without built-in accounts enabled.

Immediate Recommendations

Organizations should immediately implement the following controls:

- Disable Portal PSA accounts.
- Disable Server IAA accounts.
- Remove weak password recovery answers.
- Replace common administrator usernames with unique account names.
- Ensure the ArcGIS Enterprise service account is not assigned administrator privileges.
- Run the Security & Privacy Adviser tool available through the ArcGIS Trust Center.
- Review all built-in user accounts and remove unused accounts.
- Audit administrative accounts for unauthorized password reset activity.

Near-Term Recommendations

- Configure SMTP for secure email validation of password recovery requests.
- Prepare to deploy Esri's upcoming security patch immediately upon release.
- Verify all password recovery processes function through email validation.
- Review account recovery configurations across all ArcGIS Enterprise deployments.

Long-Term Security Recommendations

- Migrate authentication to centralized identity providers (Active Directory, Azure AD, SAML, LDAP).
- Enforce Multi-Factor Authentication (MFA) for all administrative accounts.
- Minimize or eliminate the use of built-in ArcGIS accounts.
- Regularly review ArcGIS Enterprise Hardening Guide recommendations.
- Keep ArcGIS Enterprise deployments updated with the latest security patches.
- Continuously monitor authentication logs for anomalous password reset attempts.
- Conduct periodic security assessments of authentication and account recovery configurations.

RECOMMENDATIONS:

Immediate Actions:

- Organizations using built-in ArcGIS accounts should immediately implement Esri's recommended mitigations, enable SMTP-based account validation, disable unnecessary built-in privileged accounts, and prepare to deploy the forthcoming security patch as soon as it becomes available.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/june-2026-arcgis-security-bulletin