Esri Coordinated Vulnerability Disclosure Program

Version 2.1
March 2026

Esri's Product Security Incident Response Team (PSIRT) recognizes and appreciates that our customers and the broader security community assist Esri by helping us provide safe and secure software for our customers.

Esri welcomes the contributions of security researchers and customer security assurance teams (referred to as Reporters) who coordinate sharing issues with Esri's PSIRT and help improve our products.

This document details Esri's Coordinated Vulnerability Disclosure Program overall process and reporting requirements.

Note: *The workflow in this document is specifically for reporting potential vulnerability concerns. If you believe your ArcGIS implementation has been breached/compromised, please immediately open a case with the PSIRT via the ArcGIS Trust Center.*

Contents

Overview

We encourage disclosure of security vulnerabilities that fall within our program scope and that have the potential to impact the confidentiality and integrity of datasets or the availability of Esri software offerings. Activities conducted in accordance with this process are covered under Esri's Safe Harbor provisions. To ensure prompt review and validation of a vulnerability by a member of Esri's Product Security Incident Response Team, please follow the five submittal process steps below:

1. Reporter validates eligibility and scope
2. Vulnerability is submitted via ArcGIS Trust Center
3. PSIRT reviews, validates, and communicates status
4. Fix is developed and released (if accepted)
5. Coordinated public disclosure occurs

Each of these steps are covered in detail below.

Note: If you plan to test/validate the services Esri hosts, please ensure you complete a Security Assessment Agreement (SAA) first as specified in the FAQ.

STEP 1: Validate Eligibility (Reporter)

Before anything is submitted to Esri concerning a potential security vulnerability, to reduce delays or potential rejection, please ensure the vulnerability is appropriately categorized and associated pre-requisites have been completed as follows:

Categorize Vulnerability

There are three primary types of vulnerabilities reported (CVEs, Exploits, Configuration), each of which have different submittal requirements, therefore, start by identifying the type of vulnerability:

1. CVEs

CVEs are typically detected by security scanning products of 3rd party/open-source components incorporated into our products. Unfortunately, many CVEs identified by scanners are false positives due to misidentification of components, or Esri software is not vulnerable due to how our product uses/implements the component.

2. Exploitable

Demonstratable exploits via our specific products are typically the most actionable/critical concern and receive expedited review by our PSIRT. Descriptions of demonstrable exploits are provided in well-formatted, quality reports that contain step by step instructions to reproduce a vulnerability.

3. Configuration

Some security tools don't identify CVEs, or flag demonstratable exploits with our products, but instead flag items that are not aligned with security best practices, which could lead to a more vulnerable implementation. Understanding if the issue is an Esri managed or Customer managed security configuration issue is critical, as the PSIRT only accepts Esri managed security configuration issues as potential cases.

Validate Prerequisites

Frequently, Esri has already addressed vulnerability concerns as either part of patches, new releases, or clarifications of non-exploitability, therefore we have established pre-requisites that must be addressed for different vulnerability types as follows before a report is submitted to Esri:

1. *CVE Requirements*

1.1. **CVE List** – Esri maintains a listing of 3rd party component CVE responses for our products within the ArcGIS Trust Center (an ArcGIS account is necessary to access). It is required you confirm that the CVE you would like to report is NOT already addressed in the list, nor the ArcGIS Trust Center Announcements. CVEs already addressed by Esri will be rejected for new case requests.

- Why? This eliminates unnecessary tickets for CVE's that already have confirmed responses for our products. For industry-wide, media-hyped CVE's we post announcements on the ArcGIS Trust Center for wider awareness status. Note, that foundational products from Esri have VEX files available upon request for customers, which will gradually replace the CVE listing for helping expediate validation efforts by customers.

1.2. **Product Version** - Must be validated by Reporter with latest release or Long-Term-Support (LTS) product version from Esri with all security patches in place.

- Why? Esri regularly updates third-party/open-source components as part of new releases. If you are running an older release, it WILL contain more known vulnerable CVEs over time.

1.3. **Severity** – CVEs have an associated severity score ranging from 1 to 10. Esri only accepts CVEs with a severity score of 7 or higher (which is for high and critical severity vulnerabilities).

- Why? Most third-party component CVEs are not exploitable within our products; therefore it is important to focus patching/mitigation efforts on the higher severity vulnerabilities. Moderate and lower severity vulnerabilities are typically addressed as part of a product's next release and therefore rejected for PSIRT review unless there are extenuating circumstances.
  - Exception – CVEs of concern that 1) have been identified as a Known Critical Vulnerability (KEV), 2) associated component of concern validated within our product, 3) are under General Availability or Extended support, and 4) not addressed by Esri yet, can proceed with opening a case. This exception exists to ensure Esri is appropriately addressing the potential higher risk of KEV's to customer operations.

2. *Exploitable Requirements*

2.1. **Esri Product** – Providing an exploit demonstration of a component or capability outside the use of our product is not considered valid and will be rejected as a case.

2.2. **Support Level** – Esri welcomes obtaining exploit demonstration information for any version of our products, however patches are only considered for products under General Availability or Extended Support.

3. *Configuration Requirements*

3.1. **Hardened Deployment** – Esri provides extensive security hardening guidance for foundational products within the ArcGIS Trust Center. If your deployment is NOT configured in alignment with the best practices described within our hardening guides your case will be rejected. When utilizing ArcGIS Enterprise, please refer to the ArcGIS Enterprise Hardening guide and ensure at least the Basic security profile controls are in place and perform a sanity check with the ArcGIS

Security and Privacy Adviser tool. These steps should ALWAYS be performed before any penetration test or security scans are to be performed against your systems.

3.2. **Esri vs Customer Configuration –** ArcGIS products integrate with many 3rd party products and operating systems that customers manage independent of our products. Because our products do not control these other components, shortfalls in the secure configuration of those customer managed components are not considered product security vulnerabilities. If a customer is unable to adequately secure these integrated components, we strongly recommend they consider utilizing a hosting provider or hosted service offering from Esri such as ArcGIS Online instead. Esri rejects vulnerability cases for Customer configured components/options.

STEP 2: Submit Vulnerability (Reporter)

A separate quality report should be provided for each vulnerability that meets the pre-requisite criteria as specified in Step 1. Please include the requested information listed below to help us better understand the nature and scope of the possible issue so that we can quickly triage the report. Once a report is created it should be submitted via the ArcGIS Trust Center.

NOTE: Raw, unvalidated reports from automated vulnerability scanners are rejected as typically they contain over 80% false positives.

Create Report

- **Summary** - A concise subject line describing the reported issue.
    - No longer than 1-2 sentences, briefly describing the vulnerability.
- **Vulnerability Type** – Specify if issue is a CVE, Exploit, or Configuration item.
- **Weakness Enumeration** – Specify Common Weakness Enumeration (CWE) such as CWE-120: buffer overflow.
- **Product's Affected** – List the full product name and component affected.
- **Versions Affected** – List the version detected and confirmation exists with latest product release.
- **Update Confirmation** – List all service packs, security updates, or other updates installed.
- **Configuration** - Any special/additional configuration required to reproduce the issue – must be in alignment with security hardening pre-requisites.
- **Reproduction Steps** - Step-by-step instructions to reproduce the issue on a fresh install
    - Be sure not to assume any step and attach any script or code executed in your reproduction of the issue.
    - Attachments that help in the reproduction of the report, such as images, videos, scripts, payloads, and log files are helpful.
    - Include text clearly describing what needs to be done to reproduce the report.
    - Expected result and observed result: explain how the outcome is different than what is expected.
- **Impact** - Impact of the issue, including how an attacker could exploit the issue.
- **Optional Suggestions**: Suggested remediation for bug: how would you suggest this bug is fixed?
- **Optional ID** - Additional information such as External Tracking ID.

Submit Report

To protect sensitive information and minimize risk of inadvertent disclosure, PSIRT only accepts submissions directly from customers or independent security researchers. If a customer has opened a case with Support and they determine it is a vulnerability concern, it will be handed off to PSIRT for direct engagement with the customer.

Customer-hired test teams must deliver their results exclusively to the contracting customer, who retains responsibility for submitting any security concerns to Esri.

1. Post each quality report via ArcGIS Trust Center, Report a Security or Privacy Concern page
2. If your report includes exploit details, you may want to use PGP encryption (public key here)
3. When duplicates occur, subsequent reports for same vulnerability will be marked as duplicate

STEP 3: PSIRT Validation (Esri)

Your submission will be promptly reviewed and validated by a member of Esri's PSIRT.

1. **Confirmation of receipt**
    a. An email with PSIRT ticket identifier is automatically issued to the Reporter upon receipt of submittal
        i. If you do not receive an automated response within 1 day of sending a report via the ArcGIS Trust Center, please check your junk mail for email from PSIRT@Esri.com. If that does not help, please send a high priority email direct to PSIRT@Esri.com mentioning no response was received.
2. **Validation**
    a. Depending on severity, a follow-up response is provided within hours to several days
    b. Additional information may be necessary to confirm validity/acceptance of vulnerability
3. **Notification of Acceptance or Rejection**
    a. If accepted, remediation plan information will be provided. Remediation plans could include patch plans, remediation steps, or otherwise
    b. If rejected, an explanation will be provided as to why and case closed

STEP 4: Mitigation / Patch (Esri)

Reporters wait until a fix has been made available and communicated to impacted customers, or a reasonable period has elapsed since notification prior to public disclosure.

1. **Publish CVE** - Esri is a CVE Naming Authority (CNA). CVEs will be published for Vulnerabilities that impact software deployed in a customer environment
2. **Announcement** - Security patches are posted to the ArcGIS Trust Center Announcement here.
3. **Notice** - Once a patch and associated CVE are posted, the Reporter will be notified

Note: CVEs are not issued for vulnerabilities discovered within services hosted by Esri such as ArcGIS Online, as Esri will remediate the issue and there is no action item for the customer to implement a security patch.

STEP 5: Coordinated Public Disclosure (Both)

Once the associated patch and CVE are posted, the Reporter can disclose information about the vulnerability and their role in helping identify it.

- **Timeframe** - Ideally, Reporters give customers several weeks to patch their systems before providing additional details around vulnerabilities
- **Acknowledgement** - Upon request, vulnerability Reporters are acknowledged in the ArcGIS Trust Center participating security researchers list. This program does not provide monetary rewards for bug submissions

Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct, and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy. To maintain Safe Harbor, Reporter actions must adhere to the following:

- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service.
- Performing static code analysis of Esri software is considered reverse engineering and is against Esri's terms of use.
- Do not engage in any activity that can potentially or actually cause harm to Esri, our customers, or our employees.
- Do not engage in any activity that violates (a) federal or state laws or regulations or (b) the laws or regulations of any country where (i) data, assets, or systems reside, (ii) data traffic is routed, or (iii) the researcher is conducting research activity.
- Do not store, share, compromise, or destroy Esri or customer data. If Personally Identifiable Information (PII) is encountered, you should immediately halt your activity, purge related data from your system, and immediately contact ESRI PSIRT.
    - This step protects any potentially vulnerable data, and you.
- Use your own ArcGIS accounts for testing or research purposes. Do not attempt to gain access to another user's account or confidential information.

Program Exclusions

Esri encourages any submission affecting the security of an Esri software product. However, unless evidence is provided demonstrating exploitability, the following are excluded from this program:

- Self-XSS
    - To be valid, cross-site scripting issues must be demonstrably exploitable via reflected, stored or DOM-based attacks
- Cross-Site Request Forgery resulting in logout or other low severity issues.
- Session timeout issues
    - ArcGIS Enterprise is a RESTful application. RESTful applications do not maintain session state on the server. ArcGIS Enterprise uses authorization tokens. Token timeout values are configurable as documented here
- Missing HTTP security headers (eg: Content-Security-Policy headers):
    - Esri cannot provide guidance for the specific CSP a customer may want to enforce. The number of CSP options and directives are broad and deep and highly use case dependent
    - ArcGIS Enterprise natively enforces a minimal CSP policy starting at 11.4 for Portal for ArcGIS and 11.5 for ArcGIS Server. See:
        - https://developers.arcgis.com/rest/enterprise-administration/server/update-content-security-policy/
        - https://developers.arcgis.com/rest/enterprise-administration/enterprise/security-configuration/
- Missing flags on non-sensitive cookies (locale cookies, etc)
- Password and account recovery policies, such as reset link expiration, password reset questions or password complexity
    - Password policy is user configurable
    - Esri recommends customers leverage Organization Specific logins for centralized user management
- Missing best practices in SSL/TLS configuration:
    - SSL/TLS must be configured at both the ArcGIS Enterprise and Web Server tiers
- Clickjacking/UI redressing with no practical security impact:
    - ArcGIS sets x-frame-options: SameOrigin for all OAuth requests
    - Apps and webmaps that are anonymously accessible are intended to be framed on separate domains
- Software version disclosure
    - In some cases, Esri's JS API needs to know the ArcGIS Enterprise version advertised to make determinations as to what APIs are available and supported
- Vulnerabilities in custom code developed by 3rd party vendors
- Attacks requiring a Man-in-the-Middle (MITM) or physical access to a user's device
- Vulnerabilities that require disabling security features enabled in default configurations
- Issues related to client-side password encryption
- Industry standard is to protect sensitive information using TLS

Frequently Asked Questions (FAQ's)

- **What can I do if a fix is unavailable for the ArcGIS Software version I use?**
  - This depends mostly on the Impact of the vulnerability and the Life Cycle phase in which your product is currently in. Overall, you have the following options:
    - Upgrade to a supported product version that includes a fix for this vulnerability (recommended).
    - Apply a mitigation (if one exists).
- **Why is my security scanner reporting my product as vulnerable even though my product version is marked as fixed or not affected?**
  - To maintain code stability and compatibility, Esri usually does not rebase packages to entirely new versions. Instead, we backport fixes to an older version of the software we distribute.
    - This can result in some security scanners that only consider the package version to report the package as vulnerable.
    - To avoid this, we suggest that you use an OVAL-compatible security scanner like OpenSCAP.
- **Can I perform a security assessment of services hosted by Esri such as an ArcGIS Online scan/pentest?**
  - Yes, by first submitting a Security Assessment Agreement (SAA) and receiving approval from Esri's Software Security & Privacy Team.
  - To obtain the SAA form, sent an email to SoftwareSecurity_SAA_Request@esri.com and cc your account manager.
- **My organization requires vulnerability scans to be completed, and findings addressed for new deployments of products. What is Esri's guidance for performing such scans?**
  - **Hardening**
    - Ensure the products and associated systems are hardened according to Esri guidelines
  - **Authentication**
    - When scanning ArcGIS Enterprise, users should provide the scanner with authentication details it can use to crawl the site.
      - This user should NOT be an administrative user. Leveraging a user role that does not have admin privileges prevents adverse effects related to the scanner's probing of the ArcGIS administrative APIs and other active user properties (deregistration of federated ArcGIS Servers can occur if admin accounts probe the ArcGIS Portal Admin API).
    - On a **PRODUCTION SYSTEM:** Create a "dummy" user with a "**USER" role** whose account may be modified by automated tooling instead of an active named user.
      - The intelligence of scanners for executing write functions has increased, resulting in polluting production systems with test data when a "publisher" role is utilized.
    - Instead of testing production hosts, customers may wish to configure an environment separate from production operation to prevent any potential service disruptions associated with scanning.
      - On a **NON-PRODUCTION SYSTEM:** Where the addition of test data does not matter, the Publisher account is appropriate for the vulnerability scanner to use to maximize test coverage.

- **Reporting**
    - Raw scans are not considered quality reports, while they are useful for additional context to provide as part of a case, a separate report quality report for each specific vulnerability must be provided.
    - Do not include duplicate findings for similar item types, web app templates, or services.
    - Remove common false positives including:
        - Email addresses (ex. found in our help documentation)
        - Examples of usernames may include user@domain
        - Login page password-guessing attack (5 failed attempts locks 15 min)
        - Possible internal IP disclosure (Help documents include IP address examples)
        - Possible sensitive files (Help documents accessible)
        - Exclude informational through moderate severity findings
        - Exclude findings for any libraries reporter has not validated as being used