Vulnerability Advisory

TLP: CLEAR

CAL-CSIC-2026-10-A-026

28 OCT 2026

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

# Critical SQL Injection Vulnerability in Esri ArcGIS Server for Windows and Linux

| Remote Execution | Unauthorized Data Access | No Exploitation Reported | Security Patch |
|---|---|---|---|

The Cal-CSIC has become aware of a critical SQL injection vulnerability, CVE-2026-10757, in Esri ArcGIS Server on Windows and Linux. ArcGIS Server hosts geospatial services that deliver maps and data to client applications; an attacker could use this flaw to make an accessible service invoke unauthorized database functions. The vulnerability carries a CVSS 3.1 score of 9.8.[1,2,3]

An attacker must have access to an affected ArcGIS Server service. When a service is configured with non-default public access, that access can include an anonymous remote attacker. Successful exploitation could allow the attacker to issue database-specific functions that the service should not permit.[3]

Esri released the cumulative ArcGIS Server Security 2026 Update 3 Patch on 13 October 2026 for versions 12.1, 12.0, 11.5, 11.3, and 11.1. It advises users of unlisted mature or retired releases to upgrade to a supported long-term support release; a web application firewall and the basic profile in Esri's ArcGIS Hardening Guide can reduce exposure while patching. CISA's 26 October 2026 assessment classified exploitation as 'none.' As of 28 October 2026, the vendor bulletin and official CVE record reviewed by Cal-CSIC did not identify a public proof of concept (PoC).[1,3,4]

The Cal-CSIC recommends that clients running ArcGIS Server on Windows or Linux verify whether each server has the ArcGIS Server Security 2026 Update 3 Patch and install the version-specific patch where eligible. Clients using 11.4, 11.2, or other unlisted releases should move to a supported long-term support release and apply the patch. Until remediation is complete, review service access settings, restrict unnecessary public access, and apply Esri's hardening guidance.[1,4]

For additional details regarding CVE-2026-10757, please use this link:

**Esri Security Bulletin:**

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

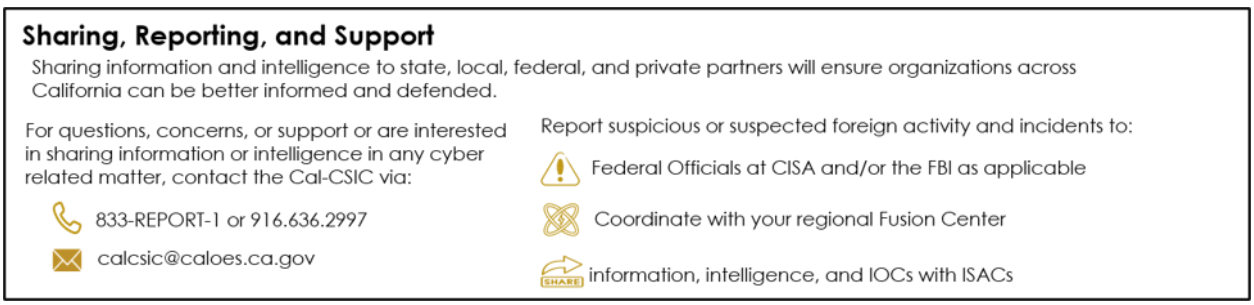
**WARNING:** This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

**Affected Products and Versions**

| Product | Affected Version | Fixed Release |
|---|---|---|
| Esri ArcGIS Server (Windows and Linux) | 12.1 | 12.1 + 2026 Update 3 Patch |
| | 12.0 | 12.0 + 2026 Update 3 Patch |
| | 11.5 | 11.5 + 2026 Update 3 Patch |
| | 11.3 | 11.3 + 2026 Update 3 Patch |
| | 11.1 | 11.1 + 2026 Update 3 Patch |
| Esri ArcGIS Server (unlisted releases) | 11.4, 11.2, or other unlisted releases | Upgrade to an eligible release; apply the patch |

*Esri's explicit patch list includes 12.1 and 11.1. The CVE record's structured range excludes 12.1, while Esri's broad '11.2 or earlier' upgrade advice includes 11.1. This table follows the version-specific patch list; unlisted releases are not patch eligible.*[1,3,4]

## Sharing, Reporting, and Support




**WARNING:** This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

## References

[1] Esri; "October 2026 ArcGIS Security Bulletin"; https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/october-2026-arcgis-security-bulletin; accessed 28 October 2026
[2] Esri; "What types of services can you publish? - ArcGIS Server"; https://enterprise.arcgis.com/en/server/10.9.1/publish-services/windows/what-types-of-services-can-you-publish.htm; accessed 28 October 2026
[3] CVE Program (Esri CNA; CISA ADP); "CVE-2026-10757 record"; https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2026/10xxx/CVE-2026-10757.json; accessed 28 October 2026
[4] Esri; "ArcGIS Server Security 2026 Update 3 Patch"; https://support.esri.com/en-us/patches-updates/2026/arcgis-server-security-2026-update-3-patch; accessed 28 October 2026

**WARNING:** This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.