



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Tuesday, July 07, 2026

CAL-CSIC-202607-A-002

Critical Path Traversal Vulnerability Impacting ESRI's ArcGIS Server

Unauthenticated Attacker

Crafted Input Paths

Access to Sensitive Data

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical path traversal vulnerability impacting ESRI's ArcGIS Server. CVE-2026-9181 carries a CVSS 3.1 score of 9.8.¹ CVE-2026-9181 enables an unauthenticated attacker to craft input paths and potentially read files not intended for public view. Successful exploitation allows a threat actor to gain access to sensitive information and configuration files on the server without credentials, potentially allowing further exploitation.²

ESRI has acknowledged this vulnerability and has published a security advisory with patch instructions.³ If patching is not immediately feasible, it is advised to block external access to the server's administrative and management interfaces and limit access to only trusted local administrators. There are no workarounds for these vulnerabilities. There is no Proof-of-Concept for CVE-2026-9181, nor is there evidence of it being exploited as a zero-day.

The Cal-CSIC recommends following ESRI's patching and workaround guidance as soon as possible. For additional details for CVE-2026-9181, please use this link:

ESRI Security Bulletin: <https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/may-2026-arcgis-security-bulletin>

Affected Products and Versions

CVE-2026-9181 impacts all versions of ESRI ArcGIS Server 12.0 and prior.

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.

TLP: CLEAR

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

¹ OpenCVE; "CVE-2026-9181"; <https://app.openCVE.io/cve/CVE-2026-9181>; accessed 07 July 2026

² HaloSecurity; "ArcGIS Server Directory Traversal Vulnerability"; <https://cve.halosecurity.com/cve-advisory/cve-2026-9181-arctgis-server-directory-traversal-vulnerability>; accessed 07 July 2026

³ ESRI; "ArcGIS Blog"; <https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/may-2026-arctgis-security-bulletin>; accessed 07 July 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.

TLP: CLEAR