Cisco Security Advisory

Cisco Slido Insecure Direct Object Reference Vulnerability

Medium

Advisory ID:
cisco-sa-slido-idor-CpsFmKxN

First Published:
2026 May 6 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwt90572

CVE-2026-20219

CWE-639

CVSS Score:
Base 5.4

Download CSAF

Email

Summary

A vulnerability in the REST API of Cisco Slido could have allowed an authenticated, remote attacker to access the social profile data of other users or affect quiz and poll results. Cisco has addressed this vulnerability in Cisco Slido and no customer action is needed.

This vulnerability existed because of the presence of an insecure direct object reference. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by sending a crafted request to the vulnerable API endpoint. A successful exploit could have allowed the attacker to view the social profiles of other users or affect quiz and poll results.

As mentioned, Cisco has addressed this vulnerability in the Slido service, and no customer action is necessary to update on-premises software or devices. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-slido-idor-CpsFmKxN

Affected Products

Vulnerable Products

This vulnerability affects Cisco Slido, which is cloud based.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

Cisco has addressed this vulnerability in Cisco Slido, which is cloud based. No user action is required.

Customers who need additional information are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

Cisco would like to thank Rafal Golabek for reporting this vulnerability.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-slido-idor-CpsFmKxN

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2026-MAY-06

Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT

The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco Technical Assistance Center (TAC). Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

When considering software upgrades, customers are advised to regularly consult the advisories for the relevant Cisco products to determine exposure and a complete upgrade solution. In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

LEGAL DISCLAIMER DETAILS

CISCO DOES NOT MAKE ANY EXPRESS OR IMPLIED GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CISCO DOES NOT GUARANTEE THE ACCURACY OR COMPLETENESS OF THIS INFORMATION. THIS DOCUMENT IS PROVIDED ON AN " AS IS" BASIS. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the Cisco Security Advisories page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the Cisco Security Vulnerability Policy for more information.

- ▶ Cisco Security Vulnerability Policy
- ▶ Subscribe to Cisco Security Notifications
- ▶ Related to This Advisory