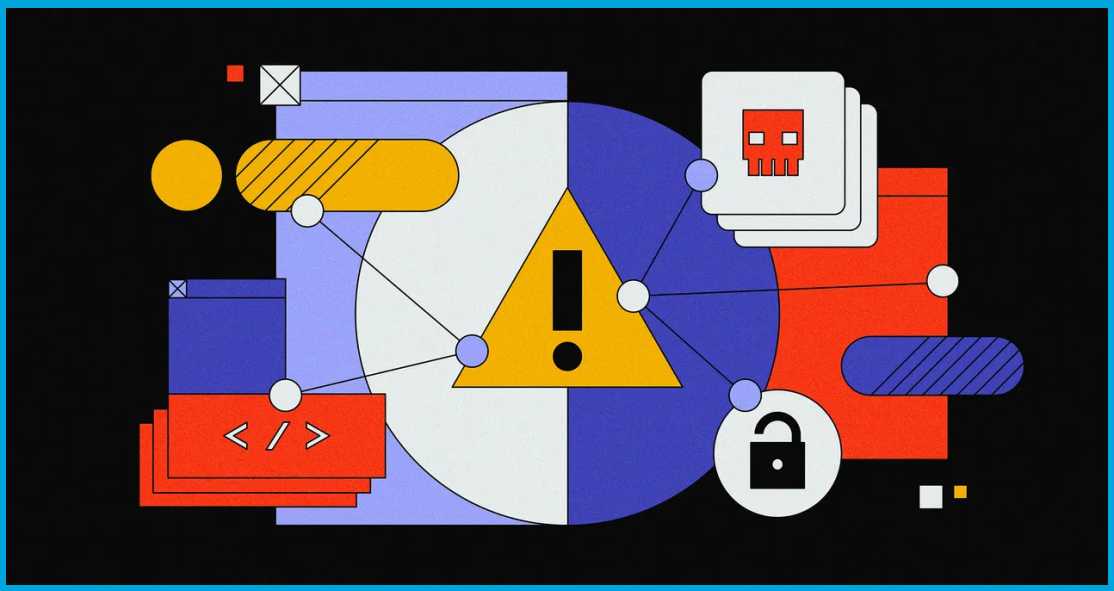
Security Newsletter

26 Sep 2022

Subscribe to this newsletter

Slack's and Teams' Lax App Security Raises Alarms



Collaboration apps like Slack and Microsoft Teams have become the connective tissue of the modern workplace, tying together users with everything from messaging to scheduling to video conference tools. But as Slack and Teams become full-blown, app-enabled operating systems of corporate productivity, one group of researchers has pointed to serious risks in what they expose to third-party programs—at the same time as they're trusted with more organizations' sensitive data than ever before.

A new study by researchers at the University of Wisconsin-Madison points to troubling gaps in the third-party app security model of both Slack and Teams, which range from a lack of review of the apps' code to default settings that allow any user to install an app for an entire workspace. And while Slack and Teams apps are at least limited by the permissions they seek approval for upon installation, the study's survey of those safeguards found that hundreds of apps' permissions would nonetheless allow them to potentially post messages as a user, hijack the functionality of other legitimate apps, or even, in a handful of cases, access content in private channels when no such permission was granted.

Read More on Wired

More #News

- UK Police arrests teen believed to be behind Uber, Rockstar hacks
- Multi-million dollar credit card fraud operation uncovered
- NSA shares guidance to help secure OT/ICS critical infrastructure
- FBI: Iranian hackers lurked in Albania's govt network for 14 months
- Okta: Credential stuffing accounts for 34% of all login attempts
- MFA Fatigue: Hackers' new favorite tactic in high-profile breaches
- Say Hello to Crazy Thin 'Deep Insert' ATM Skimmers

#Breach Log

- American Airlines learned it was breached from phishing targets
- Revolut hack exposes data of 50,000 users, fuels new phishing wave
- GTA 6 source code and videos leaked after Rockstar Games hack
- New York ambulance service discloses data breach after ransomware attack
- LastPass says hackers had internal access for four days
- Uber hacked, internal systems breached and vulnerability reports stolen
- U-Haul discloses data breach exposing customer driver licenses

#Patch Time!

- Critical Magento vulnerability targeted in new surge of attacks
- New Lenovo BIOS updates fix security bugs in hundreds of models
- Wormable Flaw, 0days Lead Sept. 2022 Patch Tuesday
- Apple fixes eighth zero-day used to hack iPhones and Macs this year
- Hackers Exploited Zero-Day RCE Vulnerability in Sophos Firewall — Patch Released

#Tech and #Tools

- The Mystery of Metador | An Unattributed Threat Hiding in Telcos, ISPs, and Universities
- Making HTTP header injection critical via response queue poisoning
- (In)Secure by Design
- Breaking Bitbucket: Pre Auth Remote Command Execution (CVE-2022-36804)
- A Guide to Improving Security Through Infrastructure-as-Code
- Introducing: CloudFox
- A technical analysis of the leaked LockBit 3.0 builder

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us