Voice phishers strike again, this time hitting Cisco

Cisco said that one of its representatives fell victim to a voice phishing attack that allowed threat actors to download profile information belonging to users of a third-party customer relationship management system.

“Our investigation has determined that the exported data primarily consisted of basic account profile information of individuals who registered for a user account on Cisco.com,” the company disclosed. Information included names, organization names, addresses, Cisco assigned user IDs, email addresses, phone numbers, and account-related metadata such as creation date.

Et tu, Cisco?

Cisco said that the breach didn’t expose customers’ confidential or proprietary information, password data, or other sensitive information. The company went on to say that investigators found no evidence that other CRM instances were compromised or that any of its products or services were affected.

Phishing attacks, particularly those relying on voice calls, have emerged as a key method for ransomware groups and other sorts of threat actors to breach defenses of some of the world’s most fortified organizations. In some cases, the threat actors behind these attacks used multiple forms of communication, including email, voice calls, push notifications, and text messages. They often devote considerable research to the attacks to make them consistent

with legitimate authentication methods used internally by the target. Some of the companies successfully compromised in such attacks include Microsoft, Okta, Nvidia, Globant, Twilio, and Twitter.

https://arstechnica.com/security/2025/08/attackers-who-phished-cisco-downloaded-user-data-from-third-party-crm/