Cisco Duo warns third-party data breach exposed SMS MFA logs

Date: 16th April 2024 | Severity: High

Summary

Cybersecurity vendor Cisco on Monday warned that hackers broke into an unidentified telephony supplier used to send. Duo MFA SMS messages and stole log data that could be used in downstream attacks.

Attack Vectors

- The notice explains that a threat actor obtained employee credentials through a phishing attack and then used those credentials to gain access to the telephony provider's systems.
- The intruder then downloaded SMS and VoIP MFA message logs associated with specific Duo accounts between March 1, 2024, and March 31, 2024.
- The provider confirmed that the threat actor did not access any contents of the messages or use their access to send messages to customers.
- However, the stolen message logs do contain data that could be used in targeted phishing attacks to gain access to sensitive information, such as corporate credentials.
- The data contained in these logs includes an employee's:
  Phone number
  Carrier
  Location data
  Date
  Time
  Message type

Recommendation

- Implementing measures to prevent similar incidents from occurring in the future and additional technical measures to further mitigate the risk associated with social engineering attacks. Aware of social engineering awareness training.
- Cisco also warns customers impacted by this breach to be vigilant against potential SMS phishing or social engineering attacks using the stolen information..

Reference Links

- https://www.bleepingcomputer.com/news/security/cisco-duo-warns-third-party-data-breach-exposed-sms-mfa-logs/