## News article

May 2024

# SMS Logs of Cisco Duo Exposed

A telephony supplier used to send MFA SMS messages was breached, exposing SMS logs.

**What happened**

Earlier this month, Cisco reported the breach of one of its suppliers which provide SMS message services for the Cisco Duo MFA application. The incident began with a phishing attack on the impacted supplier, resulting in compromised credentials. The threat actor was able to use the breached credentials to access the supplier's systems and download the SMS logs of Cisco Duo users that used MFA as an authentication method between March 1st and 31st 2024.

The downloaded logs contained phone numbers, mobile provider, location data, and metadata associated with the SMS messages, which could be used in follow-on phishing attacks against impacted users. The threat actors did not however access message contents. Cisco have contacted affected customers directly following the incident.

**Wider implications**

While in this incident the SMS message contents were not breached, and therefore there was no risk of MFA bypass, the incident does highlight security risks associated with SMS MFA. Since SMS messages are unencrypted, they are far more susceptible to interception and unauthorised access compared to alternative methods such as an authenticator app.

Furthermore, it is relatively simple for a threat actor to conduct a SIM swap attack and hijack a phone number to obtain MFA codes. SIM swap attacks involve targeting the mobile provider and attempting to trick them into registering a phone number to a new device/SIM. Since this relies of the security of a third party, this risk cannot be directly controlled or mitigated by the owner of the phone number. Since phone numbers and mobile providers were exposed in this incident, threat actors could use that information to conduct SIM swap attacks against users who they know are using SMS as their MFA method.

**Organisations should:**

- Avoid using SMS MFA wherever possible.
- Ensure they have implemented number matching MFA on all accounts to reduce the risk of account compromises. This should be supported by additional conditional access controls such as geolocation restrictions, trusted devices, and blocking risk sign-ins.

**This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.**

**Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.**

**Empower your organisation today, get in touch with one of our team members.**

**info@waterstons.com.au | 02 9160 8430**

---