SECURITY · INCIDENT ANALYSIS 2026

Cisco 2022 and Webex 2024

One breach came through a person, the other through a product. Neither needed an advanced exploit, and both have cheap, specific fixes.

Cisco, May 2022. The person route

What	Detail
Detected / disclosed	24 May 2022 / 10 August 2022, by Cisco Talos
Starting point	Work password saved in a browser profile synced to a personal Google account
MFA beaten by	Voice phishing calls plus a stream of push prompts until one was approved
Result	VPN access, new MFA devices enrolled, movement inside the network
Outcome	No ransomware deployed per Cisco. About 2.8GB of files later published

Where the chain could have been cut

1. **Password in a personal profile.** Business password manager, no sync to personal accounts.
2. **Calls from "support".** A rule everyone knows: we never ring you to approve a sign-in or read a code.
3. **Push prompts.** Number matching at minimum, passkeys for admins, lock after a few denials.
4. **New devices enrolled.** Alert the administrator whenever an MFA method is added.

MFA methods compared

Method	Stops push fatigue	Stops a fake login page
SMS code	Partly	No
Simple push, approve or deny	**No**	No
Push with number matching	Mostly	Partly
Passkeys or FIDO2 keys	**Yes**	**Yes**

The phone call made the prompt feel routine

The attacker used voice calls from people claiming to be trusted support staff so that the next approval request felt expected. **Voice security and identity security are one subject.** A clear rule, a callback habit and a better MFA method close most of this route for almost no cost.

Webex, May 2024. The product route

What	Detail
Reported by	ZEIT Online with Netzbegrünung, early May 2024
Weakness	Meeting links could be found by counting up or down from a known one
Exposed	6,000+ meetings: titles, times, invitees, some marked confidential
Fixed	Patched worldwide by 28 May 2024. Bundeswehr disconnected Webex as a precaution

Meeting settings to use

- [ ] New random meeting for anything sensitive
- [ ] Passcode on every meeting
- [ ] Lobby on, lock once everyone arrives
- [ ] PIN on dial-in access
- [ ] Generic titles for sensitive meetings
- [ ] Private calendars by default
- [ ] Record only with a reason and a retention period

What training cannot fix

- How a vendor numbers its meetings.
- Whether lookups check who is asking.
- Whether enumeration gets noticed.
- Whether you can see an access log.
- **You only control these through vendor choice.**

Questions for any communications vendor

Ask	Good answer
How do your staff sign in to systems with my data?	Phishing-resistant MFA, managed devices
What stops someone ringing support to take my account?	Verification on file, callback to registered contact
Are meeting and recording links random and controlled?	Yes, with expiry on shared links
Can I see an access log?	Sign-ins, admin changes, recording access
Which third parties touch my calls or transcripts?	A short, named list

In Australia

Essential Eight lists MFA as a core strategy and favours phishing-resistant methods for important accounts. Businesses covered by the Privacy Act must assess a suspected breach within 30 days and notify the OAIC and affected people where serious harm is likely. **Meeting metadata and call recordings can both count.**