EnCyb

Severity: Critical

Advisory Type: Security

MEXC API Key Exfiltration via Chrome Extension

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

A malicious Chrome extension secretly **creates MEXC API keys** with withdrawal access and exfiltrates them via Telegram. Stolen keys enable persistent account takeover until revoked, even after the extension is removed.

- Active Region: Global
- Affected Sector: Cryptocurrency, Financial Services
- Affected Product: MEXC
- Severity: Critical
- Published Date: January 12, 2026

TECHNICAL DETAILS

- **Target:** MEXC user accounts accessed via Google Chrome browsers with the malicious extension installed. This includes any account that navigates to the API management interface while the extension is active and the session is authenticated.
- **Root Cause:** Abuse of trusted browser extension privileges to inject scripts into an authenticated MEXC web session. Insufficient detection and restriction of malicious behavior in Chrome Web Store extensions. Client-side UI manipulation allows high-risk API permissions to be concealed from the user during key creation.
- **Prerequisite for Exploitation:** The user must install the malicious Chrome extension, grant it the requested permissions, and access the MEXC API management page while logged into an authenticated account, allowing the extension to operate within the active browser session.

INDICATORS OF COMPROMISE

TYPE	IOC
Extension Name	MEXC API Automator
Extension ID	pppdfgkfdemgfknfnhpkibbkabhghhfh
Threat Actor Web Store alias	jorjortan142
Threat Actor Email	jorjortan142@gmail[.]com
Telegram Bot Token	7534112291:AAF46jJWWo95XsRWkzcPevHW7XNo6cqKG9I
Telegram Chat ID	6526634583
Threat Actor Associated Public Accounts and Domains	x[.]com/jorjortan142 t[.]me/swapsushibot hxxps[:]//www.youtube[.]com/channel/UC22QT_xOrH9PWhORCkjGI_A swapsushi[.]net

IMPACT

- Unauthorized creation and theft of MEXC API keys with withdrawal permissions.
- Full account takeover, including trading and fund withdrawals.
- Potential complete loss of wallet balances and assets.
- Persistent attacker access until stolen API keys are revoked.
- Financial loss and compromise of user account integrity.

RECOMMENDATIONS

- Immediately audit and remove untrusted or unnecessary browser extensions.
- Revoke and rotate all existing MEXC API keys, especially those with withdrawal permissions.
- Disable API withdrawal access unless explicitly required for business operations.
- Use a dedicated, hardened browser profile or device for cryptocurrency management.
- Enforce least-privilege principles for API key permissions.

REFERENCE

- https://socket.dev/blog/malicious-chrome-extension-steals-mexc-api-keys

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com