Boletín de alerta

Boletín Nro.:
Fecha de publicación: 30/04/2026
Tema: Alerta 2026-45 Ataque cadena de sumistro SAP
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Los siguientes paquetes de SAP Cloud Application Programming Model (CAP)
  - mbt@1.2.48
  - @cap-js/db-service@2.10.1
  - @cap-js/postgres@2.2.2
  - @cap-js/sqlite@2.2.2

Descripción

Se ha identificado una campaña activa de ataque a la cadena de suministro denominada “Mini Shai Hulud”, dirigida específicamente al ecosistema SAP CAP mediante la compromisión de paquetes npm legítimos utilizados en procesos de desarrollo y despliegue.

El ataque consiste en la publicación de versiones maliciosas de paquetes ampliamente utilizados dentro del flujo de desarrollo SAP, incorporando código malicioso que se ejecuta automáticamente durante la instalación (npm install) mediante scripts de tipo preinstall .

El payload malicioso incluye múltiples etapas:

- Ejecución automática previa a la instalación completa del paquete
- Descarga de binarios externos (runtime Bun) para ejecutar código malicioso
- Implementación de un payload ofuscado encargado de robo de credenciales

Una vez ejecutado, el malware permite:

- Robo de credenciales (GitHub, npm, AWS, Azure, GCP, Kubernetes, CI/CD)
- Inserción de workflows maliciosos en repositorios GitHub para persistencia
- Publicación automática de paquetes comprometidos (comportamiento tipo worm)

- Propagación lateral a través de pipelines de desarrollo y despliegue

Adicionalmente, se ha observado que el ataque compromete el pipeline de publicación upstream, incluso abusando de integraciones automatizadas (ej. herramientas de IA/código asistido con acceso a repositorios), lo que representa un vector altamente sofisticado

Algunos IoC encontrados hasta el momento son:

- 46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09
- https://webhook.site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7
- .github/workflows/shai-hulud-workflow.yml
- Llamadas a la API de GCPsecretmanager.googleapis.com
- Consultas de registro de NPM aregistry.npmjs.org/v1/search
- Llamadas a la API de GitHubapi.github.com/repos
- Ejecución de TruffleHog con argumentosfilesystem /
- Comandos de publicación de NPM con –forcebandera
- Comandos Curl dirigidos a dominios webhook.site

Solución y mitigaciones:

Se recomiendan la siguientes acciones de forma inmediata:

- Eliminar versiones comprometidas de los paquetes afectados
- Rotar todas las credenciales expuestas, incluyendo:
- Tokens npm
- GitHub tokens
- Credenciales cloud (AWS, Azure, GCP)
- Revisar integridad de repositorios y pipelines CI/CD
- Deshabilitar ejecución automática de scripts preinstall en entornos controlados
- Implementar políticas de verificación de dependencias (SCA / SBOM) .

Información adicional:

- https://www.aikido.dev/blog/mini-shai-hulud-has-appeared
- https://cybersecuritynews.com/sap-npm-packages-compromised/
- https://www.wiz.io/blog/mini-shai-hulud-supply-chain-sap-npm

- https://www.endorlabs.com/learn/mini-shai-hulud-npm-worm-hits-sap-developer-packages