CIRCUNSTANCIAS

- **Fecha del reporte:** 2023-08-30
- **Fecha de inicio:** 2023-08-30 11:49
- **Fecha de detección:** 2023-08-30 11:52
- **Fecha de corrección:** 2023-08-30 12:28
- **Duración:** 39'

IMPACTO

Pérdida de servicio en el producto Location Identity Platform afectando a los usuarios que autentican a través de los IDP de SAML y OIDC.
Las causas de la pérdida de servicio no se han debido a ningún ciberataque dirigido ni inespecífico por lo que no se ha producido brecha de seguridad alguna.

MITIGACIÓN

Se procedió a revertir el despliegue de la versión nueva del producto y se produjo una regeneración del entorno anterior.

Se restauraron los datos del DNS anteriores a la actualización.

INCIDENCIA

El equipo responsable del despliegue se percató inmediatamente del error al ver el problema en los sistemas de monitorización.

Durante el proceso de actualización del código de los IDPs del producto se produjo la adición de una nueva entrada en los DNS corporativos.

Esta entrada en los DNS ha resultado errónea sobre los sistemas productivos lo que ha provocado que los servicios no fueran accesibles desde el exterior.

Una vez detectado el error en la configuración, se ha procedido a activar el procedimiento de reversión del despliegue que llevaba aparejado un cambio en los DNS.

Teniendo en cuenta los tiempos de propagación inherentes a los sistemas DNS la reversión ha tardado en propagarse resultando en la pérdida de servicio reportada.

LECCIONES APRENDIDAS

Los cambios en los sistemas DNS alteran el procedimiento de reversión debido a los tiempos de propagación que conllevan. El procedimiento actual de reversión no involucra downtime gracias a la realización de despliegues secuenciales con monitorización automática.

Pese a que la detección ha sido precoz y el mecanismo de reversión ha funcionado como debía, la propagación de los cambios de DNS y la posterior reversión de los mismos ha causado la pérdida de servicio.

Estos cambios de DNS no estaban correctamente recogidos en el procedimiento de reversión.

SIGUIENTES PASOS

Se va a procedimentar la reversión en los cambios de DNS teniendo en cuenta que estos también pueden resultar fallidos.

La ventana de despliegues cuando se efectúan cambios de este tipo deben de abrirse en momentos de baja utilización debido al tiempo de reversión.

También se evaluará internamente si ante cambios de este tipo se puede acelerar de alguna forma la propagación de los cambios en los DNSs corporativos.