Alerta de seguridad informática	9VSA-00051-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2019
Última revisión	20 de septiembre de 2019

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información difundida por Paloalto acerca de una vulnerabilidad crítica en Harbor que permite escalar a cualquier usuario hasta los privilegios de administrador.

Vulnerabilidad

CVE-2019-16097

Producto Afectado

El producto afectado es Harbor, un registro nativo de código abierto en la nube que almacena, firma y escanea imágenes para detectar vulnerabilidades. Harbor se integra con Docker Hub, Docker Registry, Google Container Registry y otros registros. Proporciona una GUI simple que permite a los usuarios descargar, cargar y escanear imágenes de acuerdo con sus permisos.

Impacto

Fueron observados múltiples vectores de ataque que pueden iniciarse después de obtener permisos de administrador. El atacante puede descargar todos los proyectos privados e inspeccionarlos. Pueden eliminar todas las imágenes del registro y reemplazarlas. El atacante puede crear un nuevo usuario y configurarlo para que sea administrador. Después de eso, pueden conectarse al registro de Harbor a través de la herramienta de línea de comandos Docker con las nuevas credenciales y reemplazar las imágenes actuales con cualquier cosa que deseen. Estos pueden incluir malware, cripto mineros u otros.
Afecta a las versiones 1.7.0 – 1.8.2. Las versiones 1.7.6 y 1.8.3 publicadas el pasado 18 de septiembre, incluyen las actualizaciones.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlaces

https://unit42.paloaltonetworks.com/critical-vulnerability-in-harbor-enables-privilege-escalation-from-zero-to-admin-cve-2019-16097/
https://nvd.nist.gov/vuln/detail/CVE-2019-16097
https://github.com/goharbor/harbor/commit/b6db8a8a106259ec9a2c48be8a380cb3b37cf517
https://github.com/goharbor/harbor/compare/v1.8.2...v1.9.0-rc1

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.20 12:32:57 -03'00'