BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-37
Fecha de publicación: 18/09/2024
Tema: Vulnerabilidades Críticas en Ivanti CSA CVE-2024-8963 y CVE-2024-8190
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- CSA 4.6 (todas las versiones anteriores al parche 519)

Descripción

Ivanti ha revelado una nueva vulnerabilidad crítica, esta vez en su producto Cloud Services Appliance (CSA) versión 4.6, la cual fue solucionada en el parche CSA 4.6 Patch 519 publicado el 10 de septiembre. La vulnerabilidad, identificada como **CVE-2024-8963**, permite a un atacante remoto no autenticado acceder a funcionalidades restringidas mediante una explotación exitosa.

Este riesgo se incrementa si se utiliza junto con **CVE-2024-8190** ya que el atacante podría eludir la autenticación de administrador y ejecutar comandos arbitrarios en los dispositivos afectados. La vulnerabilidad CVE-2024-8190 había sido publicada hace unos días, se trataba de una vulnerabilidad de inyección de comandos OS, pero de puntuación CVSS 7.2, ya que requería autenticación con nivel de administrador. Sin embargo, con la vulnerabilidad **CVE-2024-8963** el atacante puede conseguir evadir esa condición, combinando la explotación de ambas vulnerabilidades.

Ivanti ha confirmado casos de explotación limitada de estas vulnerabilidades y recomienda a todos los usuarios actualizar a la versión 5.0 de CSA. Es importante destacar que la versión 4.6 ha llegado al final de su vida útil y ya no recibe soporte, por lo que cualquier sistema que aún opere en esa versión está en riesgo de explotación.

Además, la Agencia de Ciberseguridad y Seguridad de Infraestructura de EE.UU. (CISA) insta a los administradores a revisar el aviso de seguridad de Ivanti y aplicar las actualizaciones necesarias para mitigar los riesgos de estas vulnerabilidades. La explotación de estas fallas puede permitir la ejecución de código remoto en los dispositivos afectados, lo que representa una seria amenaza para la seguridad empresarial.

Solución

- Actualizar inmediatamente a la versión 5.0 de Ivanti CSA para eliminar el riesgo de explotación de estas vulnerabilidades.

Información adicional:

- https://www.cisa.gov/news-events/alerts/2024/09/19/ivanti-releases-admin-bypass-security-update-cloud-services-appliance
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963?language=en_US
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190?language=en_US&_gl=1*6frqvp*_gcl_au*MTIzMDUyNTU2My4xNzE4ODgyNzE0
- https://thehackernews.com/2024/09/critical-ivanti-cloud-appliance.html?m=1

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com