BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-35
Fecha de publicación: 17/09/2024
Tema: Vulnerabilidad Crítica CVE-2024-29847 en Ivanti Endpoint Manager.
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- 2024 y 2022 SU5 de Ivanti Endpoint Manager (EPM) y versiones anteriores

Descripción

Ivanti Endpoint Manager (EPM) es una solución de gestión de puntos finales empresariales que permite la administración centralizada de dispositivos dentro de una organización.

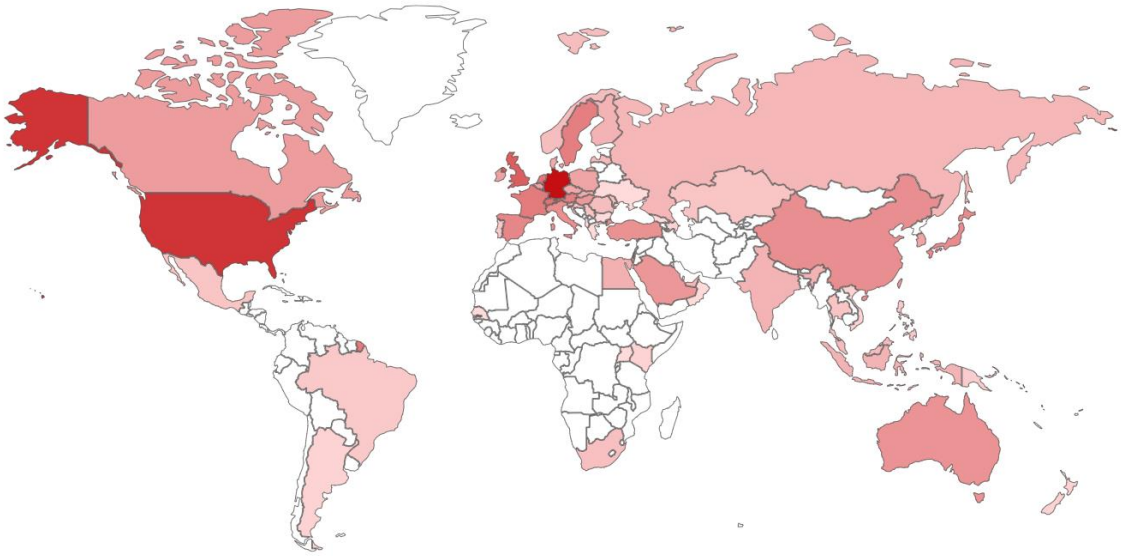
Ivanti ha publicado actualizaciones para Ivanti Endpoint Manager 2024 y 2022 SU6 que corrigen vulnerabilidades de gravedad media y alta. La explotación exitosa de estas vulnerabilidades podría permitir el acceso no autorizado al servidor central de EPM.

Una de las vulnerabilidades críticas es la CVE-2024-29847. Esta vulnerabilidad se debe a la deserialización de datos no confiables en el portal del agente de Ivanti EPM, antes de las versiones 2022 SU6 y la actualización de septiembre de 2024. Esta falla permite a un atacante remoto no autenticado ejecutar código de forma remota, con una puntuación CVSS de 10.0.

Dentro del ejecutable AgentPortal.exe, el método LANDesk.AgentPortal.AgentPortal.OnStart se invoca cada vez que se inicia el servicio "Portal del Agente". Este servicio se ejecuta de forma predeterminada, y su explotación puede permitir la ejecución remota de código no autenticado.

La vulnerabilidad radica en el uso de .NET Remoting, una tecnología que, a pesar de estar estrictamente prohibida por Microsoft debido a sus riesgos, aún se encuentra en muchas infraestructuras críticas. Gracias a .NET Remoting y a diversas técnicas, un atacante puede lograr la ejecución remota de código, lo que potencialmente permite al atacante ejecutar código completo en el servidor y manipular archivos y comandos arbitrarios

TOP COUNTRIES



Alrededor del mundo existe una aproximadamente 6000 equipos expuestos de los cuales también se sitúan en México

Solución

- Actualizar a las versiones 2024 SU1 o 2022 SU6 de Ivanti Endpoint Manager

Información adicional:

- https://summoning.team/blog/ivanti-epm-cve-2024-29847-deserialization-rce/
- https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US
- https://thehackernews.com/2024/09/ivanti-releases-urgent-security-updates.html
- https://thehackernews.com/2024/09/ivanti-warns-of-active-exploitation-of.html

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com