BOLETÍN DE ALERTA

Boletín Nro.: 2024-13
Fecha de publicación: 21/05/2024
Tema: Vulnerabilidad crítica de inyección SQL en Zabbix

Productos afectados:
Zabbix Server
-versiones desde la 6.0.0 hasta 6.0.27
-versiones desde la 6.4.0 hasta 6.4.12
-versiones desde la 7.0.0alpha1 hasta 7.0.0beta1

Descripción:

Una nueva vulnerabilidad de seguridad de severidad crítica, con número CVE-2024-22120 con una puntuación CVSSv3 de 9.1, ha sido descubierta en Zabbix, el servidor Zabbix puede realizar la ejecución de comandos para los scripts configurados, después de que se ejecuta el comando, se agrega una entrada de auditoría al "Registro de auditoría", debido a que el campo "clientip" no se sanitiza, es posible inyectar SQL en "clientip" y explotar la inyección SQL ciega basada en el tiempo.

Impacto:

Esta vulnerabilidad de inyección SQL basada en el tiempo representa un riesgo significativo para los sistemas que ejecutan versiones afectadas de Zabbix, lo que potencialmente podría permitir a un actor malicioso escalar privilegios (EoP) e incluso lograr la ejecución de código remoto (RCE).

Recomendación:

Se recomienda actualizar a la última versión de los productos afectados desde la página oficial del fabricante.

Información adicional:

- https://www.zabbix.com/la/security_advisories
- https://nvd.nist.gov/vuln/detail/CVE-2024-22120
- https://securityonline.info/cve-2024-22120-cvss-9-1-zabbix-sqli-vulnerability-exposes-it-infrastructure-to-attack/