Se revelaron múltiples vulnerabilidades en el software de monitoreo de infraestructura de TI Checkmk, que podrían ser encadenadas por un atacante remoto no autenticado para apoderarse completamente de los servidores afectados.

> *«Estas vulnerabilidades pueden ser encadenadas por un atacante remoto no autenticado para obtener la ejecución del código en el servidor que ejecuta Checkmk versión 2.1.0p10 y versiones anteriores»*, dijo Stefan Schiller, investigador de SonarSource.

La edición de código abierto de Checkmk de la herramienta de monitoreo se basa en Nagios Core y ofrece integraciones con NagVis para la visualización y generación de mapas topológicos de infraestructuras, servidores, puertos y procesos.

Según su desarrollador con sede en Múnich, tribe29 GmbH, sus ediciones Enterprise y Raw son utilizadas por más de 2000 clientes, incluyendo Airbus, Adobe, NASA, Siemens, Vodafone y otros.

Las cuatro vulnerabilidades, que consisten en dos errores críticos y dos de gravedad media, son las siguientes:

- Una vulnerabilidad de inyección de código en auth.php de watolib (puntaje CVSS: 9.1)
- Una vulnerabilidad de lectura de archivo arbitraria en NagVis (puntaje CVSS: 9.1)
- Una vulnerabilidad de inyección de comandos en el envoltorio Livestatus de Checkmk y la API de Python (puntaje CVSS: 6.8)
- Una vulnerabilidad de falsificación de solicitud del lado del servidor (SSRF) en la API de registro del host (puntaje CVSS: 5.0)

Aunque estas deficiencias por sí solas tienen un impacto limitado, un atacante puede encadenar los problemas, comenzando con la falla SSRF para acceder a un punto final solo accesible desde localhost, usándolo para eludir la autenticación y leer un archivo de configuración, y finalmente obtener acceso a la GUI de Checkmk.

> *«Este acceso se puede convertir aún más en la ejecución remota de código al explotar una vulnerabilidad de inyección de código en un subcomponente de la GUI de Checkmk llamado watolib, que genera un archivo llamado auth.php requerido para la integración de NagVis»*, dijo Schiller.

Después de la divulgación responsable el 22 de agosto de 2022, las cuatro vulnerabilidades se parchearon en la versión 2.1.0p12 de Checkmk lanzada el 15 de septiembre de 2022.

Los hallazgos siguen al descubrimiento de múltiples vulnerabilidades en otras soluciones de monitoreo como Zabbix e Icinga desde inicios de año, que podrían haberse aprovechado para comprometer los servidores mediante la ejecución de código arbitrario.