Varias redes de bots están apuntando a miles de servidores Oracle WebLogic, expuestos públicamente y aún sin parches, para implementar mineros criptográficos y robar información confidencial de sistemas infectados.

Los ataques apuntan a una vulnerabilidad del servidor WebLogic recientemente parcheada, que fue lanzada por Oracle como parte de su Actualización de Parche Crítico de Octubre de 2020, y posteriormente en noviembre (CVE-2020-14750) en forma de parche de seguridad fuera de banda.

Hasta este miércoles, fue posible acceder a unos 3 mil servidores Oracle WebLogic en Internet, según las estadísticas del motor de búsqueda Shodan.

Oracle WebLogic es una plataforma para desarrollar, implementar y ejecutar aplicaciones Java empresariales en cualquier entorno de nube, así como en las instalaciones.

La vulnerabilidad, rastreada como CVE-2020-14882, tiene una puntuación CVSS de 9.8 y afecta a las versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0 de WebLogic Server.

Aunque ya se abordó el problema, el lanzamiento del código de explotación de prueba de concepto ha convertido a las instancias vulnerables de Oracle WebLogic en un objetivo lucrativo para que los hackers recluten esos servidores en una botnet que roba datos críticos y despliegue cargas útiles de malware de segunda etapa.

Según Juniper Threat Labs, los operadores de la botnet DarkIRC están explotando la vulnerabilidad RCE para propagarse lateralmente por la red, descargar archivos, registrar pulsaciones de teclas, robar credenciales y ejecutar comandos arbitrarios en máquinas comprometidas.

El malware también actúa como un clipper de Bitcoin que les permite cambiar las direcciones de la billetera de Bitcoin copiadas en el portapapeles a la dirección de la billetera Bitcoin del operador, lo que permite a los atacantes redirigir las transacciones de Bitcoin.

Un actor de amenazas con el nombre *«Freak_OG»,* ha estado vendiendo el malware DarkIRC actualmente en foros de piratería por 75 dólares desde agosto de este año.

Pero no es solo DarkIRC el que está explotando la vulnerabilidad del servidor WebLogic. En una campaña separada, detectada por 0xrb y detallada por el investigador Tolijan Trajanovski, surgió evidencia de una botnet que se propaga por medio de la falla de WebLogic para entregar el minero de criptomonedas Monero y los binarios Tsunami.

Además de usar SSH para el movimiento lateral, se ha descubierto que la botnet logra la persistencia a través de trabajos cron, elimina las herramientas de minería de la competencia e incluso desinstala las herramientas de detección y respuesta de endpoints (EDR) de Alibaba y Tencent.

Se recomienda que los usuarios apliquen la actualización del parche crítico de octubre de 2020 y las actualizaciones asociadas con CVE-2020-14750 lo más rápido posible para mitigar los riesgos derivados de la falla.

Oracle también proporcionó instrucciones para fortalecer los servidores evitando el acceso externo a aplicaciones internas accesibles en el puerto de administración.