Se ha observado que varios atacantes utilizan de forma oportunista una vulnerabilidad de seguridad crítica ahora parcheada, que afecta a varios productos de Zoho ManageEngine desde el 20 de enero de 2023.

Rastreada como CVE-2022-47966 (puntaje CVSS: 9.8), la falla de ejecución remota de código permite una toma completa de los sistemas susceptibles por parte de los hackers no autenticados.

Hasta 24 productos diferentes, incluyendo Access Manager Plus, ADManager Plus, ADSelfServices Plus, Password Manager Pro, Remote Access Plus y Remote Monitoring and Management (RMM), se ven afectados por la vulnerabilidad.

La vulnerabilidad «*permite la ejecución remota de código no autenticado debido al uso de una dependencia de terceros obsoleta para validación de firmas XML, Apache Santuario*», dijo Martin Zugec de Bitdefender.

Según la firma rumana de seguridad cibernética, se dice que los esfuerzos de explotación comenzaron el día después de que la compañía de pruebas de penetración Horizon3.ai publicara una prueba de concepto (PoC) el mes pasado.

La mayoría de las víctimas de los ataques se encuentran en Australia, Canadá, Italia, México, Países Bajos, Nigeria, Ucrania, Reino Unido y Estados Unidos.

El objetivo principal de los ataques detectados hasta ahora gira entorno al despliegue de herramientas en hosts vulnerables como Netcat y Cobalt Strike Beacon.

Algunas intrusiones aprovecharon el acceso inicial para instalar el software AnyDesk para el acceso remoto, mientras que otras intentaron instalar una versión de Windows de una variedad de ransomware conocida como Buhti.

Además, existe evidencia de una operación de espionaje dirigida, con los hackers abusando de la vulnerabilidad de ManageEngine para implementar malware capaz de ejecutar cargas útiles de la siguiente etapa.

> *«Esta vulnerabilidad es otro claro recordatorio de la importancia de mantener los sistemas actualizados con los últimos parches de seguridad, y al mismo tiempo, emplear una fuerte defensa perimetral»*, dijo Zugec.

> *«Los atacantes no necesitan buscar nuevos exploits o técnicas novedosas cuando saben que muchas organizaciones son vulnerables a exploits anteriores debido, en parte, a la falta de una gestión adecuada de parches y riesgos».*