La Oficina Federal de Investigaciones (FBI) de Estados Unidos y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), advirtieron sobre la explotación activa de una falla recientemente parcheada en el producto ManageEngine ServiceDesk Plus de Zoho para implementar shells web y realizar una variedad de actividades maliciosas.

Rastreada como CVE-2021-44077 con puntaje CSS de 9.8, la vulnerabilidad de ejecución remota de código no autenticado afecta a las versiones de ServiceDesk Plus hasta 11305, que de no corregirse, *«permite a un atacante cargar archivos ejecutables y colocar shells web que permiten actividades posteriores a la explotación, como comprometer las credenciales de administrador, realizar movimientos laterales y filtrar colmenas de registros y archivos de Active Directory»*, dijo CISA.

> *«Una mala configuración de seguridad en ServiceDesk Plus condujo a la vulnerabilidad. Esta vulnerabilidad puede permitir que un adversario ejecute código arbitrario y lleve a cabo cualquier ataque posterior»*, dijo Zoho en un aviso independiente el 22 de noviembre.

Zoho abordó la misma vulnerabilidad en las versiones 11306 y superiores el 16 de septiembre de 2021.

CVE-2021-44077 es también la segunda falla que explota el mismo actor de amenazas que anteriormente se descubrió explotando una vulnerabilidad de seguridad en la solución de autoservicio de administración de contraseñas y de inicio de sesión único de Zoho, conocida como ManageEngine ADSelfService Plus (CVE-2021-40539) para comprometer al menos a 11 organizaciones, según un nuevo informe publicado por el equipo de inteligencia de amenazas de Unit 42 de Palo Alto Networks.

> *«El actor de amenazas expandió su enfoque más allá de ADSelfService Plus a otro software vulnerable. Más notablemente, entre el 25 de octubre y el 8 de noviembre, el actor centró su atención en varias organizaciones que ejecutan un producto de*

> *Zoho diferente conocido como ManageEngine ServiceDesk Plus»*, dijeron los investigadores Robert Falcone y Peter Renals.

Se cree que los ataques fueron orquestados por un *«actor APT persistente y decidido»* seguido por Microsoft bajo el sobrenombre de *«DEV-0322»*, un grupo de amenazas emergentes que, según la compañía, está operando en China y que anteriormente se había observado explotando una vulnerabilidad de día cero en el servicio de transferencia de archivos administrado SolarWinds Serv-U a incios del año. Unit 42 está monitoreando la actividad combinada como la campaña «TiltedTemple».

Las actividades posteriores a la explotación después de un compromiso exitoso implican que el actor cargue un nuevo cuentagotas («msiexec.exe») en los sistemas de la víctima, que luego implementa el shell web JSP en idioma chino llamado «Godzilla» para establecer la persistencia en esas máquinas, haciendo eco de tácticas similares utilizado contra el software ADSelfService.

Unit 42 identificó que en la actualidad, hay más de 4700 instancias de ServiceDesk Plus en Internet a nivel mundial, de las cuales, 2900 (62%) que abarcan Estados Unidos, India, Rusia, Gran Bretaña y Turquía, se consideran vulnerables a la explotación.

Durante los últimos tres meses, al menos dos organizaciones se han visto comprometidas al utilizar la vulnerabilidad ManageEngine ServiceDesk Plus, un número que se espera que aumente aún más a medida que el grupo APT intensifique sus actividades de reconocimiento en tecnología, energía, transporte, atención médica, educación, finanzas e industrias de defensa.

Zoho, por su parte, puso a disposición una herramienta de detección de exploits para ayudar a los clientes a identificar si sus instalaciones locales se han visto comprometidas, además de recomendar que los usuarios *«actualicen a la última versión de ServiceDesk Plus (12001) inmediatamente»* para mitigar cualquier riesgo potencial derivado de la explotación.