BOLETÍN DE ALERTA

Boletín Nro.: 2021-34

Fecha de publicación: 07/12/2021

Tema: Múltiples vulnerabilidades en diferentes aplicaciones de Zoho ManageEngine.

Fecha de actualización: 09/12/2021

Versiones afectadas:

- **CVE-2021-44515**
  - ManageEngine Desktop Central 10.1.2137.2
- **CVE-2021-44526**
  - ServiceDesk Plus versiones anteriores a 12003
- **CVE-2021-44077**
  - Zoho ManageEngine ServiceDesk Plus versiones anteriores a 11306
  - ServiceDesk Plus MSP versiones anteriores a 10530
  - SupportCenter Plus versiones anteriores a 11014
- **CVE-2021-40539**
  - ADSelfService Plus versiones anteriores a 6113

Descripción:

Se han identificado un total de cuatro fallos de seguridad que afectan a la plataforma Zoho ManageEngine, éstos pueden ser explotados por un usuario malintencionado para evadir protocolos de autenticación y/o ejecutar comandos remotamente en la máquina que posee el software instalado.

A continuación se describen las vulnerabilidades:

CVE-2021-44515 de severidad alta con una puntuación de 8.1, se debe a un problema en la autenticación de *ManageEngine Desktop Central* que permitiría a un atacante con peticiones maliciosas ejecutar código remoto en el sistema que se posee instalado el software.

CVE-2021-44526 de severidad alta (aún sin puntuación), se debe a un error al procesar las solicitudes de autenticación que permitiría a un atacante evadir los protocolos de autenticación y acceder a información confidencial tal como: archivos de configuración, los activos asociados a un usuario, entre otros.

CVE-2021-44077 de severidad critica con una puntuación de 9.8, se debe a un problema de autenticación que afecta a versiones de *ManageEngine ServiceDesk Plus* desde 11305 y

anteriores. La explotación de esta vulnerabilidad permitiría a los atacantes realizar ejecución remota de comandos sin autenticación previa.

CVE-2021-40539 de severidad critica con una puntuación de 9.8, permitiría a un atacante crear una URL de API Rest diseñada para evadir un protocolo de seguridad por medio de un error en la serialización de la URL y a su vez ejecutar código remoto en el sistema en que se encuentra instalada la aplicación sin previa autenticación.

Impacto:

La explotación de estas vulnerabilidades permitiría a un atacante comprometer la integridad de los datos, así como ejecutar código malicioso en el sistema en que se encuentra instalada la aplicación.

Solución:

Se recomienda actualizar a la versión más reciente del software instalado en el sistema, para más información ingresar en las siguientes guías:

- ZoHo advisory for CVE-2021-44515
- ZoHo advisory for CVE-2021-44526
- ZoHo advisory for CVE-2021-44077
- ZoHo advisory for CVE-2021-40539

Información adicional:

- https://www.manageengine.com/products/service-desk/security-response-plan.html
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44077
- https://us-cert.cisa.gov/ncas/current-activity/2021/12/02/cisa-and-fbi-release-alert-active-exploitation-cve-2021-44077-zoho
- https://us-cert.cisa.gov/ncas/alerts/aa21-336a
- https://nvd.nist.gov/vuln/detail/CVE-2021-44077
- https://nvd.nist.gov/vuln/detail/CVE-2021-40539
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44077
- https://nvd.nist.gov/vuln/detail/CVE-2021-40539
- https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-for-cve-2021-44526-and-cve-2021-44515-authentication-bypass-vulnerabilities-in-servicedesk-plus-and-desktop-central