Investigadores de seguridad descubrieron una nueva vulnerabilidad crítica, identificada como CVE-2020-7247, en el servidor de correo electrónico OpenSMTPD, que podría permitir a los atacantes remotos tomar el control completo sobre BSD y muchos servidores basados en Linux.

OpenSMTPD es una implementación de código abierto del protocolo SMTP del lado del servidor que se desarrolló inicialmente como parte del proyecto OpenBSD pero ahora viene preinstalado en muchos sistemas basados en UNIX.

Según Qualys Research Labs, que descubrió la vulnerabilidad, el problema reside en la función de validación de dirección del remitente de OpenSMTPD, llamada *smtp_mailaddr()*, que puede explotarse para ejecutar comandos de shell arbitrarios con privilegios de raíz elevados en un servidor vulnerable con el simple hecho de enviar SMTP especialmente diseñado.

La falla afecta a OpenBSD versión 6.6 y funciona en contra de la configuración predeterminada para ambos, la interfaz habilitada localmente y de forma remota si el daemon ha sido habilitado para escuchar en todas las interfaces y acepta correo externo.

> *«La explotación de la vulnerabilidad tenía algunas limitaciones en cuando a la longitud de la parte local (se permite un máximo de 64 caracteres) y los caracteres para escapar (‘$’, ‘|’)»,* dijeron los investigadores.
>
> *«Los investigadores de Qualys pudieron superar estas limitaciones utilizando una técnica del gusano Morris (uno de los primeros gusanos informáticos distribuidos por medio de Internet y el primero en obtener una atención importante de los medios de comunicación) al ejecutar el cuerpo del correo como un script de shell en Enviar Correo».*

Además, los investigadores también lanzaron un código de explotación de prueba de

concepto que demuestra la vulnerabilidad de OpenSMTPD. Qualys informó de forma responsable sobre la falla a los desarrolladores de OpenSMTPD, quienes publicaron hoy OpenMSTPD versión 6.6.2p1 con un parche y también presentaron una actualización para los usuarios de OpenBSD.

Se recomienda a los administradores de sistemas que ejecuten servidores con una versión vulnerable del software de correo electrónico que apliquen el parche lo más pronto posible.