Después de la divulgación sobre una vulnerabilidad crítica de día cero en Webmin la semana pasada, los encargados del mantenimiento del proyecto revelaron que la falla no fue en realidad el resultado de un error de codificación por los programadores.

A diferencia de eso, un hacker plantó en secreto una puerta trasera en algún punto de su infraestructura de construcción, que de forma sorprendente, persistió en distintos lanzamientos de Webmin (1.882 a 1.921) y finalmente permaneció oculto por más de un año.

Con más de 3 millones de descargas al año, Webmin es una de las aplicaciones basadas en web de código abierto más populares del mundo para administrar sistemas basados en Unix, como servidores Linux, FreeBSD y OpenBSD.

Webmin ofrece una interfaz de usuario (UI) simple para administrar usuarios y grupos, bases de datos, BIND, Apache, Postfix, Sendmail, QMail, copias de seguridad, firewalls, monitoreo y alertas y más.

La historia comenzó cuando el investigador turco Özkan Mustafa Akkus, presentó públicamente una vulnerabilidad de ejecución remota de código 0-day en Webmin, en DefCon, el pasado 10 de agosto, sin avisar previamente a los responsables del proyecto que fueron afectados.

> *«No recibimos ninguna notificación previa, lo cual es inusual y poco ético por parte del investigador que lo descubrió. Pero, en tales casos, no podemos hacer nada más que arreglarlo lo antes posible»,* dijo Joe Cooper, uno de los desarrolladores del proyecto.

Además de revelar la falla al público, Akkus también lanzó un módulo Metasploit para dicha vulnerabilidad, que tiene como objetivo automatizar la explotación utilizando el framework de Metasploit.

La vulnerabilidad, identificada como CVE-2019-15107, se introdujo en una característica de

seguridad diseñada para permitir que el administrador de Webmin aplique una política de caducidad de contraseña para las cuentas de otros usuarios.

Según el investigador, la falla de seguridad reside en la página de restablecimiento de contraseña y permite que un atacante remoto no autenticado ejecute comandos arbitrarios con privilegios de root en los servidores afectados simplemente agregando un comando pipe («|») en el antiguo campo de contraseña por medio de peticiones POST.

Cooper mencionó en una publicación que el equipo sigue investigando cómo y cuándo se introdujo la backdoor, pero confirmó que las descargas oficiales de Webmin fueron reemplazadas por los paquetes retroactivos solo en el repositorio SourceForge del proyecto, y no en los repositorios GitHub de Webmin.

Cooper también hizo hincapié en que la función de caducidad de la contraseña afectada no se habilita de forma predeterminada para las cuentas de Webmin, lo que significa que la mayoría de las versiones no son vulnerables en su configuración predeterminada, y la falla solo afecta a los administradores de Webmin que habilitaron de forma manual dicha función.

> *«Para explotar el código malicioso, se debe tener en la instalación Webmin > Configuración de Webmin > Autenticación > Política de caducidad de contraseña configurada, para solicitar a los usuarios con contraseñas caducadas que ingresen una nueva. Esta opción no está configurada de forma predeterminada, pero si está configurada, permite la ejecución remota de código»*, agregó Cooper.

Sin embargo, otro investigador de seguridad en Twitter, reveló que la versión 1.890 de Webmin se ve afectada en la configuración predeterminada, ya que los hackers parecen haber modificado el código fuente para habilitar la función de caducidad de contraseña de forma predeterminada para todos los usuarios de Webmin.

Estos cambios inusuales en el código fuente de Webmin fueron marcados por un administrador a fines del año pasado, pero los desarrolladores de Webmin nunca

sospecharon que no fue su error, aunque finalmente el código fue modificado por otra persona de forma intencional.

Según una búsqueda de Shodan, Webmin tiene más de 218,000 instancias expuestas a Internet disponibles en este momento, ubicadas principalmente en Estados Unidos, Francia y Alemania, de las cuales, más de 13 mil instancias ejecutan Webmin vulnerables versión 1.890.

Los desarrolladores de Webmin han eliminado la puerta trasera maliciosa en su software para abordar la vulnerabilidad y lanzaron versiones limpias, Webmin 1.930 y Usermin versión 1.780.

Los últimos lanzamientos de Webmin y Usermin también abordan muchas vulnerabilidades de scripting entre sitios (XSS) que fueron reveladas responsablemente por un investigador de seguridad que ya fue recompensado.