Se han descubierto varias vulnerabilidades de seguridad en el paquete needrestart, incluido por defecto en Ubuntu Server desde la versión 21.04. Estas fallas, que han estado presentes durante más de una década, permiten a un atacante local obtener privilegios de administrador (root) sin requerir la intervención del usuario.

El equipo de investigación de amenazas de Qualys (TRU, por sus siglas en inglés), que reportó estas vulnerabilidades el mes pasado, señaló que son fáciles de aprovechar, por lo que instó a los usuarios a instalar los parches disponibles de inmediato. Según los análisis, estas vulnerabilidades existen desde la introducción del soporte para intérpretes en la versión needrestart 0.8, lanzada el 27 de abril de 2014.

> *«Las fallas en needrestart posibilitan la escalada de privilegios locales (LPE), permitiendo que un atacante local obtenga acceso root. Las vulnerabilidades afectan a distribuciones como Debian, Ubuntu y otras basadas en Linux»*, explicó Ubuntu en su comunicado, donde también mencionó que el problema se solucionó en la versión 3.8.

Needrestart es una herramienta que identifica qué servicios deben reiniciarse tras aplicar actualizaciones de bibliotecas compartidas, minimizando la necesidad de un reinicio completo del sistema.

Detalles de las vulnerabilidades:

1. CVE-2024-48990 (puntuación CVSS: 7.8): permite a un atacante ejecutar código como root engañando a needrestart para que utilice un intérprete de Python manipulado mediante una variable de entorno PYTHONPATH controlada por el atacante.
2. CVE-2024-48991 (puntuación CVSS: 7.8): un fallo que posibilita que un atacante, aprovechando una condición de carrera, haga que needrestart ejecute un intérprete de Python falso bajo su control.
3. CVE-2024-48992 (puntuación CVSS: 7.8): un error que facilita la ejecución de código como root mediante el uso de una variable de entorno RUBYLIB maliciosamente

manipulada para ejecutar un intérprete de Ruby comprometido.

4. CVE-2024-11003 (puntuación CVSS: 7.8) y CVE-2024-10224 (puntuación CVSS: 5.3): vulnerabilidades que pueden ser explotadas para ejecutar comandos de shell arbitrarios como root al aprovecharse de problemas en el paquete libmodule-scandeps-perl (versiones anteriores a la 1.36).

Si se explotan con éxito, estas fallas permiten que un atacante local manipule variables de entorno como PYTHONPATH o RUBYLIB, lo que resulta en la ejecución de código arbitrario cuando se ejecuta needrestart.

Ubuntu destacó:

> *«En CVE-2024-10224, un atacante puede suministrar entradas maliciosas al módulo Perl Module::ScanDeps, lo que podría llevar a la ejecución de comandos de shell al abrir un 'pipe' malicioso (por ejemplo, pasando 'commands|') o al ejecutar cadenas arbitrarias mediante eval().*
> *Además, en CVE-2024-11003, needrestart pasa entradas manipuladas (nombres de archivos) al módulo Module::ScanDeps, lo que desencadena el CVE-2024-10224 con privilegios de root. La solución elimina la dependencia de needrestart de Module::ScanDeps«.*

Aunque la recomendación principal es instalar las actualizaciones más recientes, Ubuntu sugirió como medida temporal desactivar los escáneres de intérpretes en el archivo de configuración de needrestart y restaurar esta funcionalidad tras aplicar los parches.

> *«Las vulnerabilidades en needrestart permiten a usuarios locales ejecutar código malicioso con privilegios elevados durante instalaciones o actualizaciones de paquetes, cuando este programa generalmente se ejecuta como root»*, explicó Saeed Abbasi, gerente de producto en Qualys TRU.

> *«Explotar estas fallas podría otorgar acceso completo como root al atacante, comprometiendo la seguridad y estabilidad del sistema».*