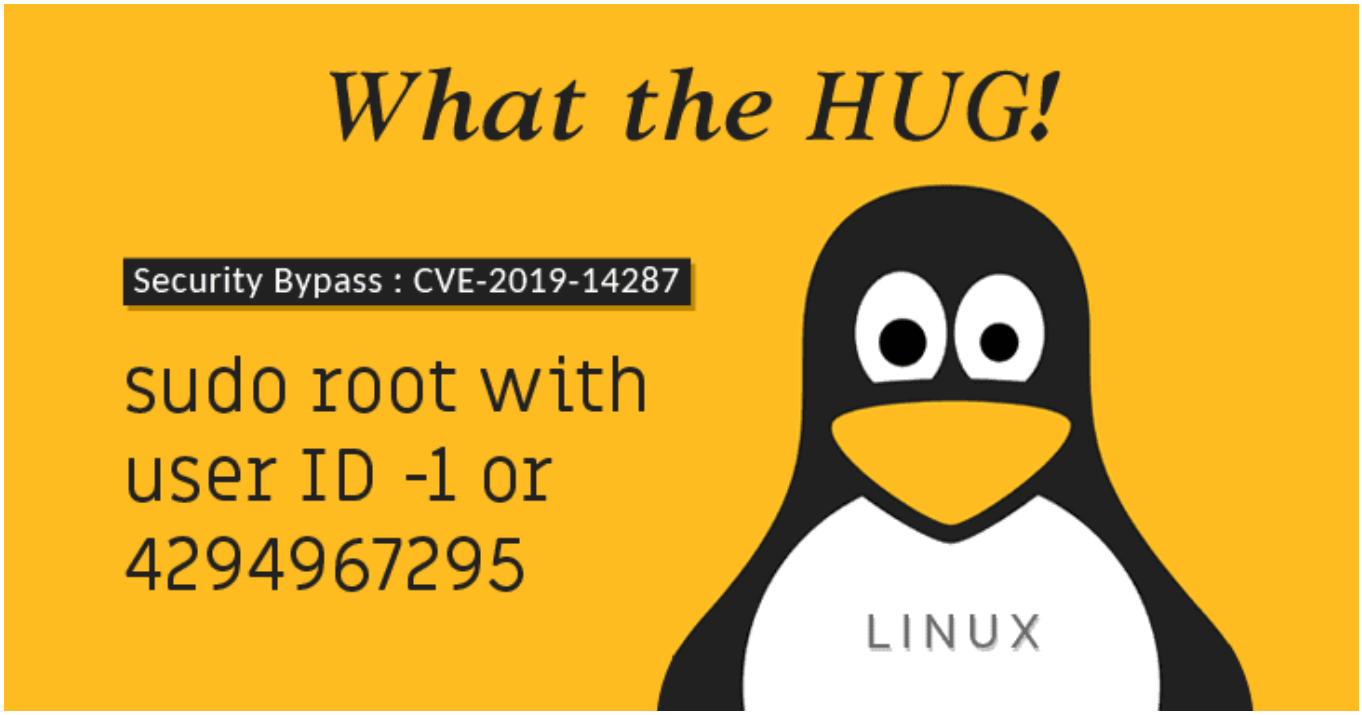
الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

الهيئة الوطنية لخدمات الشبكة
National Agency for Network Services

ثغرة في sudo تسمح لمستخدمي Linux بتنفيذ الأوامر بصلاحيات root



إعداد

قسورة ع. عيسى

تم اكتشاف ثغرة أمنية جديدة في Sudo – إحدى أهم الأدوات المساعدة والأكثر استخداماً والتي تأتي بمثابة أداة أساسية مثبتة على كل نظام تشغيل مبني على نظامي التشغيل UNIX و Linux تقريباً.

تكمن الثغرة في إمكانية تخطّي سياسة الأمان في أداة sudo والتي يمكن أن تسمح لمستخدم أو برنامج خبيث بتنفيذ أوامر اختيارية بصلاحيات root على نظام Linux حتى عندما تمنع عدادات "sudoers" الحصول على صلاحيات root.

Sudo تعني "super user do"، هو أمر نظام يسمح للمستخدم بتشغيل التطبيقات أو الأوامر بصلاحيات مستخدم آخر دون تبديل البيئات – عادة لتشغيل الأوامر كمستخدم root.

بشكل افتراضي، في معظم توزيعات Linux، تسمح الكلمة المفتاحية (ALL) في إعدادات RunAs في ملف /etc/sudoers، كما هو موضح في الصورة أدناه، لجميع المستخدمين في مجموعتي admin أو sudo بتشغيل أي أمر باسم أي مستخدم آخر على النظام.

```
# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
ninja@saffron:~$
```

على أي حال، نظراً لأن الفصل بين الصلاحيات هو أحد نماذج الأمان الأساسية في Linux، يمكن للمسؤولين إنشاء ملف sudoers لتحديد المستخدمين الذين يمكنهم تشغيل الأوامر التي يحددها المستخدمون.

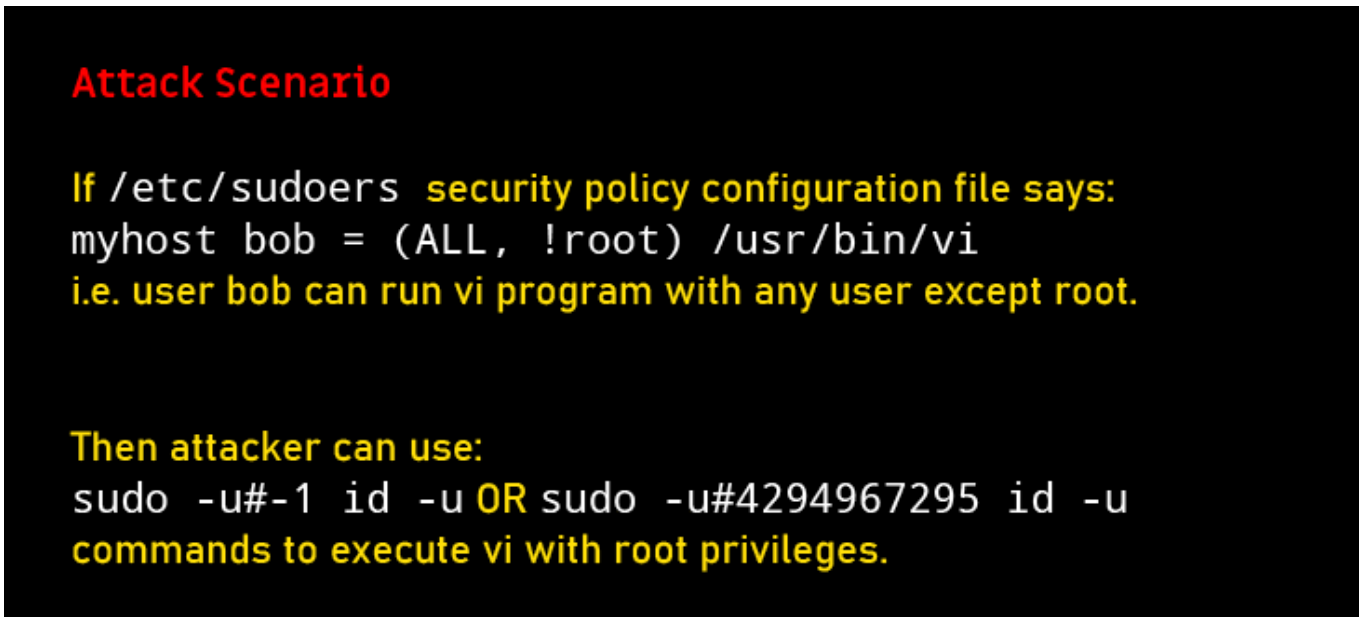
لذا، في سيناريو معين، حيث يُسمح لك بتشغيل أمر محدد، أو أي أمر على الإطلاق، كمستخدم آخر باستثناء مستخدم root، تسمح لك هذه الثغرة بتجاوز سياسة الأمان هذه والتحكم الكامل في النظام كمستخدم root.

كيفية استغلال هذه الثغرة؟

الثغرة، المعرفة بالرقم CVE-2019-14287، والتي اكتشفها Joe Vennix أحد موظفي قسم أمن المعلومات في شركة Apple، تعتبر خطيرة لأن أداة sudo صُممت للسماح للمستخدمين باستخدام كلمة المرور الخاصة بهم لتنفيذ الأوامر كمستخدم مختلف دون الحاجة إلى كلمة المرور لذلك المستخدم.

وما يزيد خطورة هذه الثغرة هو أنها تسمح للمهاجمين بتشغيل الأوامر كمستخدم root فقط عن طريق تحديد معرف المستخدم أو الـID كـ -1 أو 4294967295.

يعود ذلك إلى قيام الدالة (function which converts) التي تحول معرف المستخدم (user id) إلى اسم المستخدم (user name) والتي تعامل الرقم -1 أو القيمة العادلة له في نطاق الأرقام الطبيعية (بدون إشارة) 4294967295 وكأنهما الرقم 0، والذي يعتبر دائماً معرف المستخدم الخاص بـ root.



بالإضافة إلى ذلك، ولأن معرف المستخدم المحدد عبر الخيار u- غير موجود في قاعدة بيانات كلمات المرور، فلن يتم تشغيل أي وحدات PAM لجلسة العمل."

تؤثر الثغرة على جميع إصدارات Sudo قبل أحدث إصدار تم طرحه والذي يحمل الرقم 1.8.28، والذي تم إصداره من أيام قليلة جداً ، وسيتم طرحه قريباً كتحديث بواسطة توزيعات Linux المختلفة لمستخدميها.

نظرًا لأن الهجوم يعمل في سيناريو حالة استخدام محدد لملف الإعدادات sudoers ، فلا ينبغي أن يؤثر على عدد كبير من المستخدمين ، ومع ذلك ، إذا كنت تستخدم Linux ، فلا يزال يوصى بشدة بتحديث حزمة sudo إلى أحدث إصدار.

المصادر:

https://nvd.nist.gov/vuln/detail/CVE-2019-14287

https://thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html

https://www.sudo.ws/stable.html

https://www.sudo.ws/repos/sudo/rev/83db8dba09e7