[TLP: WHITE]
Krytyczna podatność CVE-2021-3156 w Sudo

Zespół CERT Polska rekomenduje administratorom systemów operacyjnych Linux (Ubuntu, Debian, Fedora, Gentoo i inne), aby niezwłocznie zaaplikowali poprawkę naprawiającą krytyczną podatność w paczce "sudo" (CVE-2021-3156).

Podatność

Narzędzie sudo niepoprawnie przetwarza dane wejściowe pochodzące od użytkownika, co skutkuje występowaniem błędu przepełnienia bufora na stercie (ang. *Heap-based Buffer Overflow*). W domyślnej konfiguracji dowolny użytkownik w systemie, posługując się odpowiednio spreparowaną komendą, może dokonać eskalacji uprawnień do poziomu administratora ("root") i w konsekwencji przejąć kontrolę nad systemem operacyjnym.

Test podatności

Obecność podatności w systemie operacyjnym można sprawdzić poprzez wywołanie następującego polecenia:

```
sudoedit -s '\' `perl -e 'print "A" x 65536'`
```

Polecenie może zostać uruchomione z poziomu konta dowolnego użytkownika bądź konta administratora.

Interpretacja wyniku:

- jeżeli wystąpi błąd wykonywania programu (np.: *"Segmentation fault"*, *"Aborted (core dumped)"*, *"malloc(): corrupted top size"*), oznacza to, że używana wersja paczki sudo **jest podatna na CVE-2021-3156**;
- jeżeli zostanie wypisana pomoc programu sudoedit (*usage: sudoedit (...)*) - używana wersja paczki sudo **nie jest podatna**;

Poprawka

Należy niezwłocznie zaktualizować pakiet "sudo". Wspierane wersje dystrybucji systemów operacyjnych Ubuntu, Debian, Fedora oraz Gentoo otrzymały stosowną poprawkę bezpieczeństwa. Poprawkę można otrzymać poprzez aktualizację pakietu sudo za pomocą standardowego oficjalnego kanału aktualizacji.

Ubuntu/Debian:
```
apt-get update && apt-get --only-upgrade install sudo
```

Fedora:
```
yum update sudo
```

W przypadku innych systemów wykorzystujących program sudo należy podjąć próbę aktualizacji oficjalnym kanałem, a w przypadku braku stosownej poprawki skontaktować się z dystrybutorem systemu.

Więcej informacji

Dokładne szczegóły techniczne na temat podatności zostały opublikowane przez firmę Qualys, która ujawniła występowanie podatności[1]. Informacje o podatności są również dostępne w bazie MITRE pod numerem CVE 2021-3156[2].

1 https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit

2 https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3156

ul. Kolska 12, 01-045 Warszawa

tel.: +48 22 380 82 74
fax: +48 22 380 83 99

Zgłaszanie incydentów: cert@cert.pl
e-mail: info@cert.pl

/CERT.Polska
@CERT_Polska

www.cert.pl
www.nask.pl