NOTIFIKASI INDIKASI KERENTANAN UBUNTU OVERLAYFS LOCAL PRIVILEGE ESCALATION CVE-2021-3493

RINGKASAN EKSEKUTIF

1. Badan Siber dan Sandi Negara (BSSN) menginformasikan adanya *tools exploit* yang memanfaatkan kerentanan Ubuntu Overlays CVE-2021-3492 pada versi:
   - Ubuntu 20.10
   - Ubuntu 20.04 LTS
   - Ubuntu 18.04 LTS
   - Ubuntu 16.04 LTS
   - Ubuntu 14.04 LTS ESM

   Kerentanan ini mulai dipublikasikan oleh Ubuntu pada tanggal 15 April 2021. Pihak Ubuntu menyampaikan bahwa kerentanan CVE tersebut tergolong **high** karena memungkinkan *user* lokal ubuntu mendapatkan akses *root privileges*. Kerentan ini disebabkan oleh implementasi OverlayFS di kernel Linux yang tidak memvalidasi penggunaan *namespaces* dengan baik.
2. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan ini dan kode serangan yang telah tersebar secara umum (https://github.com/briskets/CVE-2021-3493/blob/main/exploit.c), diharapkan para pengguna Ubuntu dengan versi yang telah disebutkan sebelumnya untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

ANALISIS

1. Penjelasan Umum

CVE-2021-3493 merupakan kerentanan pada sistem operasi Ubuntu yang memanfaatkan proses OverlayFS untuk menggabungkan bebepa *mount* menjadi *union mounting* pada kernel sehingga pengguna dapat mengakses semua *file* tersebut dalam satu struktur direktori dan mendapatkan akses *root privileges*. Pada dasarnya overlay memiliki 2 bagian, *upper layer* yang memiliki *file permission read-write* dan *lower layer* yang memiliki *file permission read-only*. Dengan menggunakan overlay, user akan mendapatkan *permission read-write* pada *file* di kedua layer tersebut namun tidak sebagai *root* melainkan hanya mendapatkan *permission* akses pada komponen yang diperlukan untuk mengakses *file* tersebut. Eksploitasi pada CVE ini dilakukan dengan menggunakan sebuah kode yang mampu memanfaat celah pada overlay. Setelah informasi kerentanan ini dirilis, kode eksploit terhadap kerentanan ini telah tersebar luas secara umum. Kode yang digunakan telah disesuaikan dengan komponen yang diperlukan untuk mendapatkan akses root sehingga ketika eksploitasi kode tersebut berhasil maka user penyerang mendapatkan akses privilege sebagai root. Informasi kerentanan ini pertama kali terdaftar pada 12 April 2021 oleh NVD (National Vulnerability Database) dan secara resmi di umumkan oleh pihak Ubuntu pada 15 April 2021. Berdasarkan NVD dan CVSS, kerentanan dengan kode CVE-2021-3493 memiliki nilai **7.8** yang dikategorikan sebagai kerentanan **high**. Produk

yang terdampak dari kerentanan CVE-2021-3493 adalah Ubuntu versi 20.10,20.04 LTS,18.04 LTS,16.04 LTS, dan 14.04 ESM.

2. Analisis Kerentanan

Sistem operasi Linux mendukung *file capabilities* yang tersimpan di atribut file tambahan yang cara kerjanya hampir mirip dengan setuid-bit. Dibawah ini merupakan kode prosedur yang disederhanakan untuk mengatur *file capabilities*.

```
setxattr(...):
    if cap_convert_nscap(...) is not OK:
        then fail
    vfs_setxattr(...)
```

Fungsi pemanggilan yang paling penting pada kode tersebut adalah `cap_convert_nscap`. Fungsi tersebut berfungsi untuk melakukan pengecekan *permission* dari tiap *namespaces.* Jika user mengatur *file capabilities* dari namespaces dan mount miliknya, tidak akan menjadi masalah karena user memang memiliki akses tersebut. Masalah terjadi ketika OverlayFS meneruskan operasi tersebut melalui underlying file system, operasi tersebut hanya akan memanggil `vfs_setxattr` dan melewati fungsi `cap_convert_nscap` sehingga memungkinkan user dapat sewenang-wenang mengganti *file capabilities* diluar namespaces dari user tersebut.

REKOMENDASI

Sebagai langkah pencegahan terhadap kerentanan yang ada, Direktorat Operasi Keamanan Siber BSSN mengimbau kepada para pengguna sistem operasi Ubuntu dengan versi yang telah disebutkan agar segera melakukan langkah langkah mitigasi dibawah ini:

- Melakukan *update* patch kernel linux sesuai dengan arahan dari pihak Ubuntu. (https://ubuntu.com/security/notices/USN-4916-1) (https://ubuntu.com/security/notices/USN-4917-1) (https://ubuntu.com/security/notices/USN-4915-1)
- Melakukan *update* sistem operasi Ubuntu ke versi terbaru (Ubuntu 21.10) yang dapat diunduh pada link dibawah ini. (https://ubuntu.com/download/desktop/thank-you?version=21.10&architecture=amd64)