ANALISIS KERENTANAN CVE-2025-6019 PADA LIBBLOCKDEV LINUX MENGGUNAKAN PENDEKATAN VULNERABILITY ASSESSMENT

Ardhan Dimas Nuryadin, Alam Rahamtulloh
Teknik Informatika, Universitas Siliwangi
Mugarsari, Tamansari, Tasikmalaya, Indonesia
alam@unsil.ac.id

ABSTRAK

Sistem operasi Linux merupakan salah satu fondasi utama dalam infrastruktur komputasi modern, sehingga keamanan setiap komponen intinya menjadi aspek yang sangat krusial. Salah satu ancaman yang paling sering muncul pada ekosistem ini adalah Local Privilege Escalation (LPE), di mana pengguna dengan hak terbatas dapat memperoleh akses administratif penuh melalui celah logika dalam sistem. Penelitian ini menyajikan studi kasus teknis mengenai kerentanan CVE-2025-6019, sebuah celah LPE yang ditemukan pada pustaka libblockdev, yang berperan penting dalam manajemen perangkat blok dan diakses melalui layanan udisks2 dan Polkit. Dengan menggunakan pendekatan Vulnerability Assessment, penelitian ini menilai karakteristik teknis, tingkat risiko, serta efektivitas mitigasi yang diterapkan vendor. Data dianalisis dari sumber resmi seperti Red Hat Security Advisory, Bugzilla, dan National Vulnerability Database (NVD), disertai verifikasi empiris melalui Proof-of-Concept (PoC) pada lingkungan terisolasi. Hasil penelitian menunjukkan bahwa kerentanan ini memungkinkan pengguna lokal mengeksekusi berkas SUID-root melalui mekanisme mount udisks2 tanpa validasi hak akses yang memadai, sehingga menghasilkan eskalasi hak ke konteks root. Berdasarkan perhitungan CVSS v3.1, kerentanan ini dikategorikan High Severity dengan skor 7.0, berdampak pada kerahasiaan, integritas, dan ketersediaan sistem.

Kata kunci : *keamanan siber, local privilege escalation, analisis kerentanan, libblockdev, Linux.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang sangat cepat telah mendorong sistem operasi berbasis Linux menjadi salah satu platform paling banyak digunakan di berbagai sektor baik perusahaan ataupun kepemerintahan, mulai dari perangkat server hingga infrastruktur teknologi informasi, hingga IoT. Lingkungan berbasis Linux dikenal karena stabilitas, fleksibilitas, dan sifatnya yang terbuka, sehingga menjadi fondasi utama dalam pengembangan layanan digital modern. Keamanan sistem operasi modern merupakan salah satu aspek paling krusial dalam bidang teknologi informasi, mengingat sistem operasi menjadi fondasi utama bagi seluruh aktivitas komputasi dan penyimpanan data digital [1]. Berbagai survei dan tinjauan literatur menunjukkan bahwa peningkatan jumlah kerentanan (vulnerabilities) dalam perangkat lunak bersifat sejalan dengan meningkatnya kompleksitas sistem dan dependensi antarkomponen [1][2][3]. Dalam konteks ini, pendekatan Vulnerability Assessment berperan penting untuk mengidentifikasi, menilai, dan memitigasi potensi kerentanan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab [3][4]. Kerangka kerja seperti Common Vulnerability Scoring System (CVSS) juga telah digunakan secara luas sebagai standar internasional dalam mengukur tingkat keparahan risiko keamanan [5][6]. Studi-studi terdahulu menekankan bahwa analisis berbasis advisory dan evaluasi kuantitatif risiko adalah elemen kunci untuk mempertahankan ketahanan sistem terhadap eksploitasi [2][6].

Salah satu tantangan utama dalam pengelolaan keamanan sistem operasi adalah meningkatnya kompleksitas interaksi antar komponen internal seperti privilege controller, yang dapat menimbulkan celah eskalasi hak akses (privilege escalation) [7][8]. Sejumlah penelitian sebelumnya menunjukkan bahwa kesalahan kecil dalam validasi hak akses atau logika kontrol dapat menyebabkan pengguna tanpa hak istimewa memperoleh akses administratif (root access) [9]. Misalnya, studi oleh Kerutt menganalisis CVE-2024-38063 pada sistem operasi Windows dan menemukan bahwa cacat logika sederhana pada modul IPv6 dapat menghasilkan kondisi heap overflow yang memungkinkan eksekusi kode arbitrer di tingkat kernel [10]. Kerentanan jenis ini berdampak langsung pada integritas, kerahasiaan, dan ketersediaan sistem, menjadikannya area yang sangat penting untuk dikaji [5][1].

Berdasarkan laporan terbaru dari Red Hat dan NIST, ditemukan kerentanan baru yang terdaftar sebagai CVE-2025-6019, senuah kerentanan Local Privilege Escalation (LPE) pada komponen libblockdev melalui interaksi dengan udisks2 dan Polkit [5][7]. Mekanisme eksploitasi ini memungkinkan pengguna lokal dengan sesi allow_active untuk melakukan mount terhadap citra (filesystem image) berbahaya yang mengandung berkas SUID, sehingga sistem menjalankannya dengan hak akses root. Sejalan dengan penelitian Kerutt yang menekankan pentingnya analisis patch untuk menghindari potensi rollback atau reaktivasi jalur kode lama [10], maka diperlukan kajian khusus untuk menilai efektivitas mitigasi terhadap CVE-2025-6019 secara sistematis.

Penelitian sebelumnya berfokus pada root cause analysis berbasis proof-of-concept exploit [10][9], namun masih terdapat kesenjangan (research gap)

pada aspek evaluasi risiko yang komprehensif tanpa melakukan eksploitasi langsung. Dalam konteks akademik dan profesional, pendekatan yang berlandaskan pada Vulnerability Assessment dan analisis berbasis advisory dianggap lebih aman dan etis [2][4]. Berdasarkan celah tersebut, penelitian ini mengusulkan analisis mendalam terhadap CVE-2025-6019 menggunakan metode Vulnerability Assessment, dengan memanfaatkan data dari vendor advisory, serta evaluasi risiko melalui perhitungan skor CVSS v3.1.

Berdasarkan identifikasi masalah dan kesenjangan penelitian tersebut, Penelitian ini bertujuan untuk memberikan penilaian risiko yang objektif serta rekomendasi mitigasi berbasis kebijakan sistem yang dapat digunakan oleh administrator keamanan maupun pengembang distribusi Linux. Pertanyaan penelitian utama yang diangkat dalam studi ini meliputi:

a. Bagaimana karakteristik teknis dan dampak kerentanan CVE-2025-6019 terhadap sistem operasi Linux,
b. Seberapa tinggi tingkat risiko yang dihasilkan berdasarkan perhitungan CVSS, dan
c. Sejauh mana mitigasi vendor efektif dalam menutup potensi eskalasi hak akses.

Penelitian ini diharapkan dapat menghasilkan hasil analisis dan model mitigasi yang mampu memetakan pola serangan terhadap pustaka sistem dan memberikan rekomendasi mitigasi adaptif sesuai karakteristik ancaman. Hasil kajian ini diharapkan memperkuat literatur keamanan sistem operasi dan memberikan kontribusi praktis terhadap upaya pencegahan eksploitasi Local Privilege Escalation pada sistem berbasis Linux.

Secara keseluruhan, hasil utama penelitian ini menunjukkan bahwa kerentanan CVE-2025-6019 memiliki skor risiko tinggi (CVSS 7.0) dengan dampak penuh terhadap kerahasiaan, integritas, dan ketersediaan sistem apabila tidak diterapkan pembatasan kebijakan mount dan kontrol Polkit secara ketat. Analisis patch dari Red Hat dan NVD menunjukkan bahwa versi terbaru libblockdev telah menutup celah tersebut, meskipun masih memerlukan konfigurasi keamanan tambahan seperti penerapan SELinux dan AppArmor. Penelitian ini disusun dengan struktur sebagai berikut: Bagian 1 Pendahuluan; Bagian 2 menjelaskan metodologi penelitian; Bagian 3 membahas hasil analisis dan perancangan strategi mitigasi; dan Bagian 4 menyimpulkan temuan utama serta arah penelitian lanjutan.

2. TINJAUAN PUSTAKA

2.1. Keamanan Sistem Operasi dan Kerentanan Perangkat Lunak

Keamanan sistem operasi merupakan elemen fundamental dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Sejumlah penelitian sebelumnya menyatakan bahwa meningkatnya kompleksitas perangkat lunak mendorong bertambahnya jumlah kerentanan yang dapat dieksploitasi oleh pihak tidak berwenang [1][2]. Selain itu, efektivitas manajemen patch dianggap sangat berpengaruh dalam mencegah eksploitasi berulang, terutama pada sistem yang memiliki banyak dependensi internal [1].

Penelitian terkait analisis kerentanan juga menyoroti pentingnya proses vulnerability assessment sebagai metode untuk mengidentifikasi, menilai, dan memberikan mitigasi terhadap potensi ancaman tanpa melakukan eksploitasi langsung pada sistem produksi [3][4]. Pada berbagai studi, pendekatan ini digunakan untuk menilai risiko secara sistematis berdasarkan standar pengukuran internasional seperti CVSS.

2.2. Local Privilege Escalation (LPE)

Local Privilege Escalation (LPE) adalah salah satu kategori kerentanan yang paling banyak ditemukan dalam sistem operasi modern. LPE memungkinkan pengguna biasa memperoleh hak administratif akibat kesalahan validasi akses atau cacat logika pada modul tertentu [5]. Contohnya, menunjukkan bahwa kelemahan kecil pada modul IPv6 di Windows dapat menyebabkan heap overflow yang memungkinkan eksekusi kode arbitrer di tingkat kernel [10]. Temuan-temuan seperti ini menegaskan bahwa LPE sangat kritis karena berdampak pada ketiga aspek CIA: kerahasiaan, integritas, dan ketersediaan.

2.3. Polkit, udisks2, dan libblockdev sebagai Komponen Middleware Linux

Polkit merupakan komponen kontrol akses penting pada sistem Linux yang berfungsi menentukan izin tindakan administratif berdasarkan sesi pengguna. Beberapa penelitian dan dokumentasi teknis menunjukkan bahwa konfigurasi Polkit, khususnya allow_active, menjadi area sensitif karena dapat memengaruhi siapa yang diizinkan menjalankan operasi privileged melalui D-Bus [7].

Di sisi lain, udisks2 merupakan daemon manajemen media yang beroperasi dengan hak root untuk menangani mount, resize, dan manipulasi filesystem lainnya. udisks2 memanfaatkan pustaka libblockdev sebagai backend untuk mengelola operasi perangkat blok. Studi-studi dari komunitas keamanan dan vendor seperti Red Hat dan SOC Prime membahas bagaimana interaksi ketiga komponen tersebut dapat membuka peluang celah eskalasi hak akses apabila validasi input atau kebijakan sesi tidak dikonfigurasi dengan benar [5][7][8].

2.4. Penelitian Terdahulu mengenai Kerentanan Pada Middleware Linux

Beberapa penelitian sebelumnya menyoroti bahwa middleware berbasis D-Bus sering menjadi target eskalasi hak akses karena ia menjadi perantara antara user-space dan root-service [8]. Analisis dari Snyk Labs dan komunitas keamanan lainnya menjelaskan pola umum eksploitasi, seperti:

a. memanfaatkan operasi filesystem yang berjalan sebagai root,
b. menyisipkan artefak berbahaya dalam image atau media virtual,
c. dan memanfaatkan kebijakan Polkit yang longgar.

Studi-studi tersebut memberi dasar teoretis bahwa kombinasi kesalahan validasi dan hak istimewa otomatis pada middleware dapat menciptakan permukaan serangan LPE.

2.5. Kerentanan CVE-2025-6019

CVE-2025-6019 merupakan bagian dari kategori LPE yang melibatkan komponen libblockdev dan udisks2. Vendor advisory dari Red Hat, NVD, dan laporan komunitas menunjukkan bahwa celah ini muncul karena ketidaktepatan validasi hak akses pada operasi mount atau resize filesystem yang dipicu oleh pengguna aktif melalui D-Bus [5][7][8]. Celah ini memungkinkan file SUID berbahaya dieksekusi dengan konteks root setelah image filesystem dimount secara otomatis oleh udisks2.

Penelitian-penelitian sebelumnya yang membahas mekanisme serupa mendukung argumen bahwa eksploitasi melalui filesystem image merupakan teknik yang realistis dan berbahaya, terutama pada sistem multi-user. Oleh karena itu, temuan pada CVE-2025-6019 konsisten dengan pola ancaman LPE yang telah dikaji dalam literatur terdahulu, sekaligus memperluas pemahaman mengenai risiko pada middleware penyimpanan Linux.

3. METODE PENELITIAN

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan deskriptif analitis dengan metode Vulnerability Assessment sebagai kerangka utama analisis. Metode ini digunakan untuk menilai dan mengevaluasi tingkat risiko keamanan dari suatu kerentanan perangkat lunak berdasarkan data sekunder yang diperoleh dari vendor advisory, basis data keamanan publik, dan laporan teknis terpercaya.

Selain menggunakan sumber resmi, penelitian ini juga memanfaatkan dokumen Security Advisory CVE-2025-6019 yang disusun oleh peneliti sendiri sebagai salah satu rujukan analisis. Dokumen tersebut berisi hasil kompilasi dan interpretasi terhadap berbagai sumber publik yang relevan, serta berfungsi sebagai bahan pendukung dalam proses identifikasi kerentanan dan penyusunan rekomendasi mitigasi.

Pendekatan ini dipilih karena sesuai untuk penelitian non-eksperimental yang berfokus pada analisis risiko dan mitigasi tanpa perlu melakukan eksploitasi langsung terhadap sistem target, yang bukan hanya berfungsi sebagai informasi akademis, namun dapat digunakan sebagai Security Advisory sebagai Vendor Perusahaan Managed Security Services Providers (MSSP).

3.2. Lokasi dan Sumber Data Penelitian

Penelitian ini menggunakan pendekatan deskriptif analitis dengan metode Vulnerability Assessment sebagai kerangka utama analisis. Metode ini digunakan untuk menilai dan mengevaluasi tingkat risiko keamanan dari suatu kerentanan perangkat lunak berdasarkan data sekunder yang diperoleh dari vendor advisory, basis data keamanan publik, dan laporan teknis terpercaya.

Salah satu referensi analisis yang digunakan adalah Security Advisory CVE-2025-6019 yang disusun oleh peneliti, yang mengintegrasikan informasi teknis dari berbagai vendor dan komunitas keamanan.

Data penelitian ini bersifat sekunder, diperoleh dari sumber-sumber publik dan vendor resmi. Adapun sumber utama yang digunakan meliputi:

a. Security Advisory CVE-2025-6019 (disusun oleh peneliti sendiri).
b. Red Hat Product Security Portal, melalui laporan RHSA-2025:9328 yang menjelaskan patch dan mitigasi terhadap CVE-2025-6019.
c. National Vulnerability Database (NVD), yang menyediakan deskripsi teknis, vektor CVSS, dan skor risiko resmi untuk CVE-2025-6019.
d. Bugzilla Red Hat (issue tracker) yang memuat diskusi teknis, patch commit, dan timeline pelaporan / perbaikan terkait bug id 2370051.
e. Artikel teknis dan blog komunitas yang memberikan konteks implementasi D-Bus / Polkit dan pola eskalasi hak akses, antara lain tulisan pengantar tentang D-Bus & Polkit dan analisis abuse case pada distribusi Ubuntu.
f. SOC Prime Threat Detection Labs dan laporan komunitas lain yang memberikan analisis tambahan terkait potensi eksploitasi Local Privilege Escalation pada udisks2 dan libblockdev.
g. Laporan dan sumber dokumentasi vendor (Red Hat advisories, NVD) yang digunakan untuk memverifikasi versi terdampak, tanggal rilis patch, serta rekomendasi mitigasi resmi.

Penggunaan sumber-sumber ini memungkinkan analisis yang transparan dan dapat direplikasi tanpa melakukan eksperimen intrusif pada sistem nyata.

3.3. Tahapan Penelitian

Metodologi penelitian ini disusun mengikuti empat tahapan utama berdasarkan model Vulnerability Management Lifecycle, seperti yang ditunjukkan pada Gambar 1 berikut:

Gambar 1. Vulnerability management lifecycle

3.4. Identifikasi Kerentanan

Tahap awal dilakukan untuk mengidentifikasi kerentanan target, yaitu CVE-2025-6019, dengan mengumpulkan seluruh informasi terkait dari Berdasarkan advisory peneliti, CVE-2025-6019 diidentifikasi sebagai LPE pada pustaka libblockdev akibat kesalahan validasi hak akses allow_active pada Polkit. Peneliti juga mencari informasi dari NVD, CVE MITRE, Red Hat Advisory, serta Bugzilla Red Hat. Langkah-langkah yang dilakukan meliputi:

a. Menentukan ruang lingkup komponen terdampak (libblockdev, udisks2, dan Polkit).
b. Menganalisis deskripsi CVE, tingkat keparahan, serta lingkungan operasional yang berisiko.
c. Mengidentifikasi versi Linux yang terdampak dan potensi eksploitasi melalui sesi allow_active.

Hasil dari tahap ini berupa profil lengkap kerentanan CVE-2025-6019 yang berisi vektor serangan, mekanisme eksploitasi, dan cakupan sistem terdampak.

3.5. Analisis Teknis (Technical Analysis)

Tahap ini bertujuan untuk memahami mekanisme internal yang menyebabkan terjadinya Local Privilege Escalation. Analisis dilakukan dengan meninjau cara kerja modul udisks2 dalam memanggil pustaka libblockdev serta bagaimana Polkit mengatur kebijakan hak akses pengguna aktif. Tahapan analisis ini meliputi:

a. Penelaahan perubahan kode berdasarkan patch log Red Hat dan diskusi di Bugzilla.
b. Analisis konfigurasi kebijakan Polkit dan alur komunikasi D-Bus berdasarkan dokumentasi u1f383 (2025).
c. Pembandingan dengan temuan dari Snyk Labs (2025) mengenai eksploitasi serupa pada sistem Ubuntu.

Analisis teknis ini membantu menjelaskan penyebab logis (logical flaw) yang memungkinkan pengguna non-root mendapatkan akses administratif di sistem Linux.

3.6. Evaluasi Risiko

Evaluasi risiko dilakukan menggunakan kerangka kerja CVSS v3.1 untuk menentukan tingkat keparahan kerentanan. Penilaian mencakup beberapa parameter seperti:

a. Attack Vector (AV) — lokal atau jaringan,
b. Attack Complexity (AC) — kompleksitas serangan,
c. Privileges Required (PR) — tingkat hak akses awal,
d. User Interaction (UI) — keterlibatan pengguna,
e. serta dampak terhadap Confidentiality (C), Integrity (I), dan Availability (A).

Perhitungan skor CVSS dilakukan dengan mengacu pada data NVD, Red Hat, CVE MITRE, serta sumber lainnya yang mendukung, kemudian dibandingkan untuk memastikan konsistensi klasifikasi risiko.

Interpretasi hasil dibagi ke dalam kategori Low, Medium, High, dan Critical, dengan pembahasan mendalam mengenai kontribusi setiap metrik terhadap skor akhir.

3.7. Analisis Mitigasi (*Mitigation Analysis*)

Tahap akhir difokuskan pada evaluasi efektivitas mitigasi yang diterapkan vendor dalam mengatasi CVE-2025-6019. Analisis dilakukan dengan:

a. Menelaah patch resmi Red Hat, validasinya melalui Bugzilla, serta sumber lainnya yang mendukung.
b. Menganalisis potensi rollback vulnerability.
c. Mengkaji rekomendasi untuk memastikan perlindungan berlapis terhadap kerentanan LPE.

Tahapan ini menghasilkan rekomendasi mitigasi adaptif yang dapat diterapkan oleh administrator sistem untuk memperkuat keamanan pada lingkungan Linux.

3.8. Metode Analisis Data

Analisis data dilakukan secara deskriptif kualitatif dengan dukungan evaluasi kuantitatif melalui skor CVSS. Tahapan analisis mencakup:

a. Deskripsi Kerentanan: menguraikan mekanisme CVE-2025-6019 berdasarkan vendor advisory dan dokumentasi teknis.
b. Evaluasi Risiko: menghitung skor CVSS v3.1 untuk menentukan tingkat keparahan.
c. Analisis Komparatif: membandingkan hasil evaluasi dengan studi sebelumnya.
d. Rekomendasi Mitigasi: menyusun strategi mitigasi adaptif berbasis policy configuration dan least privilege principle.

3.9. Proof-of-Concept

Pelaksanaan Proof-of-Concept (PoC) yang dimanfaatkan untuk memverifikasi alur eskalasi hak akses yang diidentifikasi pada CVE-2025-6019. Semua pengujian PoC dilaksanakan pada satu perangkat milik peneliti dalam lingkungan yang terisolasi dan terkendali; tidak ada sistem pihak ketiga yang menjadi target maupun skenario attacker–victim yang melibatkan infrastruktur eksternal. Tujuan utama pelaksanaan PoC adalah mereproduksi kondisi di mana sebuah image filesystem berisi artefak beratribut istimewa (misalnya berkas SUID) diproses oleh komponen manajemen media sehingga berpotensi menghasilkan eksekusi dengan hak istimewa root.

3.10. Etika Penelitian

Penelitian ini mematuhi prinsip Responsible Disclosure dan Non-Intrusive Research, di mana seluruh aktivitas analisis dilakukan tanpa mengubah, menguji, atau mengeksploitasi sistem produksi. Semua data bersifat publik dan digunakan hanya untuk kepentingan akademik dengan mencantumkan sumber secara jelas.

4. HASIL DAN PEMBAHASAN

4.1. Gambaran Umum kerentanan

Kerentanan CVE-2025-6019 dikategorikan sebagai celah untuk *Local Privilege Escalation* (LPE) pada sistem operasi berbasis Linux. Celah ini ditemukan pada pustaka libblockdev, yang merupakan bagian dari infrastruktur manajemen blok penyimpanan dan digunakan oleh udisks2 untuk menjalankan operasi mount dengan hak akses administratif.

Masalah utama muncul pada mekanisme interaksi antara udisks2 dan Polkit, khususnya pada parameter allow_active, yang digunakan untuk menentukan apakah sesi pengguna aktif memiliki izin untuk menjalankan perintah tertentu. Dalam versi terdampak, fungsi ini tidak memverifikasi hak akses pengguna secara ketat, sehingga pengguna lokal dapat membuat filesystem image berbahaya berisi berkas SUID-root shell, lalu meminta udisks2 untuk melakukan mount terhadap citra tersebut.

Ketika proses mount dilakukan, *daemon udisks2* menjalankan operasi tersebut dengan hak administratif penuh (*root privileges*), memungkinkan pengguna non-root mengeksekusi berkas SUID tersebut dan memperoleh akses sistem penuh. Berdasarkan laporan *Red Hat Security Advisory* RHSA-2025:9328, CVE MITRE, dan *National Vulnerability Database* (NVD), kerentanan ini diklasifikasikan dengan tingkat keparahan atau *severity High* (CVSS v3.1 score: 7.0) dan memengaruhi berbagai distribusi Linux seperti *RHEL, Fedora, dan CentOS Stream*.

4.2. Analisis Mekanisme Serangan

Berdasarkan hasil analisis teknis yang terdokumentasi dalam Security Advisory CVE-2025-6019, serta dokumentasi mengenai kerentanan udisks2 dan libblockdev, akar penyebab kerentanan ini adalah kesalahan dalam logika kontrol akses antara *udisks2*, *libblockdev*, dan *Polkit.*

Vurnerability ini memungkinkan penyerang untuk mengeksploitasi Local Privilege Escalation (LPE) yang memanfaatkan cara udisks2 dan libblockdev menangani proses mount image file sistem. Dalam serangan ini, penyerang yang hanya memiliki akses sebagai user biasa dapat membuat sebuah *image* berformat XFS yang berisi file berstatus SUID-root, seperti *shell.* Kemudian, penyerang meminta sistem untuk melakukan mount terhadap image tersebut menggunakan udisks2, yang secara default dijalankan dengan hak akses root tanpa memverifikasi keamanan isi image secara menyeluruh. Setelah image berhasil dimount, file SUID di dalamnya dapat dijalankan oleh penyerang dan akan dieksekusi dengan hak akses root.

Dengan teknik ini, penyerang berhasil mendapatkan akses penuh ke sistem, memungkinkan pencurian data, modifikasi sistem, atau sabotase layanan. Dengan demikian, pola kelemahan ini termasuk dalam kategori *logical privilege misvalidation*, di mana fungsi keamanan yang semestinya melindungi justru dapat dimanfaatkan untuk eskalasi hak akses.

4.3. Evaluasi Risiko Berdasarkan CVSSv3

Penilaian risiko dilakukan menggunakan kerangka kerja Common Vulnerability Scoring System (CVSS v3.1) berdasarkan data yang diperoleh dari NVD dan verifikasi silang terhadap vendor advisory Red Hat. Skor yang didapat dari kerentanan ini sebesar 7.0 dengan tingkat *severity* nya *High*. Parameter-parameter penilaian risiko untuk CVE-2025-6019 ditunjukkan pada Tabel 1.

Tabel 1. Evaluasi Risiko CVE-2025-6019 Berdasarkan CVSS v3.1

Parameter	Nilai	Keterangan
Attack Vector (AV)	Local	Eksploitasi memerlukan akses fisik atau sesi pengguna lokal
Attack Complexity (AC)	Low	Eksploitasi tidak membutuhkan kondisi khusus
Privileges Required (PR)	Low	Dapat dilakukan oleh pengguna biasa
User Interaction (UI)	None	Tidak memerlukan keterlibatan pengguna lain
Scope (S)	Unchanged	Eksploitasi tidak memengaruhi konteks keamanan lain
Confidentiality (C)	High	Dapat membaca seluruh data sistem
Integrity (I)	High	Dapat memodifikasi konfigurasi dan file sistem
Availability (A)	High	Dapat mengganggu layanan dan proses penting
Skor CVSS v3.1 (NVD)	7.0 (High Severity)	Risiko tinggi terhadap sistem lokal

Analisis terhadap vektor CVSS menunjukkan bahwa kombinasi antara *Privileges Required = Low* dan *Attack Complexity = Low* menjadikan kerentanan ini sangat berisiko pada sistem yang digunakan oleh beberapa pengguna (*multi-user environment*).

Kerentanan ini memberikan peluang bagi pengguna biasa untuk memperoleh akses administratif penuh tanpa memerlukan exploit kompleks, hanya dengan memanfaatkan konfigurasi Polkit yang longgar.

4.4. Hasil Proof-of-Concept

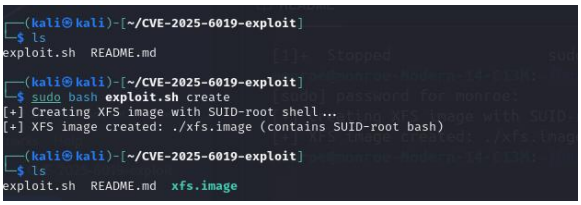
Untuk memperkuat pemahaman mekanisme pemanfaatan, penelitian ini menggunakan PoC yang tersedia pada repositori And-oss/CVE-2025-6019-exploit sebagai referensi untuk menggambarkan skenario pemanfaatan dan hanya mengeksekusi file tersebut tanpa melakukan modifikasi fungsional. Setiap langkah dan output dicatat untuk tujuan verifikasi. Adapun lingkungan pengujian terdiri dari berikut:

Tabel 2. Lingkungan penelitian

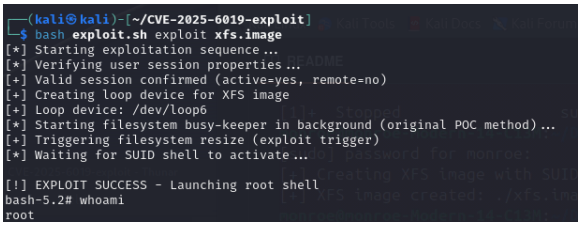
Komponen / Item	Nilai
Sistem	Lenovo Ideapad Gaming 3
Sistem Operasi	Kali GNU/Linux Rolling 2023.4 (Vmware)
RAM	16 GB
Storage	512 GB
PoC Reposity	https://github.com/And-oss/CVE-2025-6019-exploit

Pelaksanaan eksperimen dilaksanakan pada mesin uji lokal milik peneliti yang dipisahkan dari jaringan produksi. Repositori diunduh ke lingkungan pengujian dan berkas exploit.sh diinspeksi terlebih dahulu untuk memahami rangkaian perintah yang dijalankan. Setelah verifikasi isi skrip, berkas tersebut diberi izin eksekusi dan dijalankan sesuai instruksi asli; setiap perintah dan keluaran terminal direkam secara kronologis.

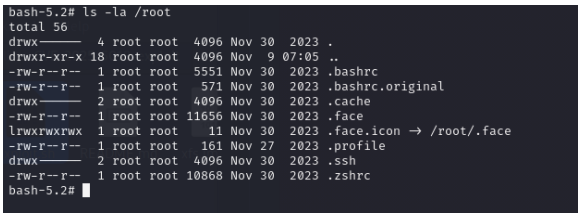
Gambar 2. Kondisi Privileges sebelum dieksploitasi



Gambar 3. persiapan dan pembuatan image XFS berisi SUID-root



Gambar 4. Eksekusi exploit dan bukti whoami berubah menjadi root



Gambar 5. Percobaan akses direktori /root setelah eskalasi

Gambar 6. Verifikasi kondisi non-root sebelum eskalasi (tidak dapat mengakses /root)

PoC membuktikan bahwa CVE-2025-6019 memungkinkan eskalasi hak lokal melalui race condition pada udisks2 saat melakukan resize filesystem: dengan menyisipkan binari SUID ke image filesystem dan memicu Filesystem.Resize via DBus dalam sesi logind lokal, penyerang dapat memperoleh shell dengan effective UID root. Keberhasilan sangat tergantung pada konteks session/polkit dan konfigurasi target. Semua pengujian dilakukan pada perangkat milik peneliti dan tidak ditujukan untuk disalahgunakan.

Hasil empiris dari pelaksanaan PoC mengindikasikan bahwa pada konfigurasi yang diuji, jalur eksploitasi yang diilustrasikan oleh PoC konsisten dengan deskripsi teknis advisory. Setelah image dimount oleh udisks2, berkas yang memiliki bit SUID di dalam image dapat dieksekusi sehingga menghasilkan perubahan konteks pengguna pada shell yang diperoleh. Verifikasi ddengan memasukan perintah whoami menunjukkan konteks root pada percobaan yang berhasil. Analisis terhadap temuan ini menggarisbawahi keterkaitan teknis antara kondisi sesion Polkit (allow_active), mekanisme mount oleh udisks2, dan kemampuan file SUID untuk dieksekusi setelah mount.

5. KESIMPULAN DAN SARAN

Penelitian ini menganalisis kerentanan CVE-2025-6019 pada pustaka libblockdev menggunakan pendekatan Vulnerability Assessment berbasis advisory vendor dan verifikasi PoC pada lingkungan terisolasi, dan menunjukkan bahwa cacat logika validasi hak akses pada interaksi udisks2–libblockdev dengan kebijakan Polkit (allow_active) memungkinkan pengguna lokal mengeksekusi berkas SUID dari image filesystem yang dimount daemon udisks2 hingga memperoleh hak root dengan skor risiko CVSS v3.1 sebesar 7,0 (High) yang berdampak pada kerahasiaan, integritas, dan ketersediaan sistem, khususnya pada lingkungan multi-user dan sistem dengan fitur auto-mount. Untuk itu, administrator sistem disarankan segera menerapkan patch libblockdev/udisks2 sesuai advisory resmi, memperketat kebijakan Polkit, menonaktifkan auto-mount media tidak tepercaya, serta mengaktifkan mekanisme Mandatory Access Control (SELinux/AppArmor) dan monitoring berkala terhadap aktivitas mencurigakan terkait image filesystem dan atribut SUID. Penelitian lanjutan dapat difokuskan pada pemodelan risiko yang menggabungkan data advisory dengan telemetry operasional serta perluasan kajian ke subsistem middleware lain seperti D-Bus, PAM, dan systemd guna memperkuat ketahanan keamanan sistem Linux secara menyeluruh.

DAFTAR PUSTAKA

[1] Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management-A systematic literature review of

challenges, approaches, tools and practices. *Information and Software Technology*, *144*, 106771.

[2] Krause, H. (2025). *An Information Security Advisory Risk Assessment Concept* (Doctoral dissertation, Hochschule für Angewandte Wissenschaften Hamburg).

[3] Longueira-Romero, Á., Iglesias, R., Flores, J. L., & Garitano, I. (2022). A novel model for vulnerability analysis through enhanced directed graphs and quantitative metrics. *Sensors*, *22*(6), 2126.

[4] Du, X., Chen, B., Li, Y., Guo, J., Zhou, Y., Liu, Y., & Jiang, Y. (2019, May). Leopard: Identifying vulnerable code for vulnerability assessment through program metrics. In *2019 IEEE/ACM 41st international conference on software engineering (ICSE)* (pp. 60-71). IEEE.

[5] National Vulnerability Database (NVD), "CVE-2025-6019 – Local Privilege Escalation in libblockdev via udisks2," U.S. National Institute of Standards and Technology (NIST).

[6] Yoon, S. S., Kim, D. Y., Kim, K. K., & Euom, I. C. (2023). Vulnerability exploitation risk assessment based on offensive security approach. *Applied Sciences*, *13*(22), 12180.

[7] Red Hat Security Advisory, "RHSA-2025:9328 – Security Update for libblockdev (CVE-2025-6019)," Red Hat Product Security Portal.

[8] SOC Prime Threat Detection Labs, "CVE-2025-6018 and CVE-2025-6019 – Linux LPE Vulnerabilities in udisks2," SOC Prime Blog.

[9] M. Hutchins, "Remotely Exploiting the Kernel via IPv6 - CVE-2024-38063." [Online]. Available: https://malwaretech.com/2024/08/exploiting-CVE-2024-38063.html

[10] Kerutt, B., Lorenz, B., Schwarz, M., Kaven, S., & Skwarek, V. (2025, August). Critical analysis of CVE-2024-38063: the Microsoft IPv6-vulnerability. In *Proceedings of the International Conference on Networked Systems 2025 (NetSys 2025): Technische Universität Ilmenau, 1–4 September 2025* (pp. 5-8).