IMBAUAN KEAMANAN KERENTANAN *USE-AFTER-FREE LEAD TO PRIVILEGE ESCALATION* PADA LINUX KERNEL 5.18.1 (CVE-2022-32250)

Jumat, 26 Agustus 2022

Ringkasan Eksekutif

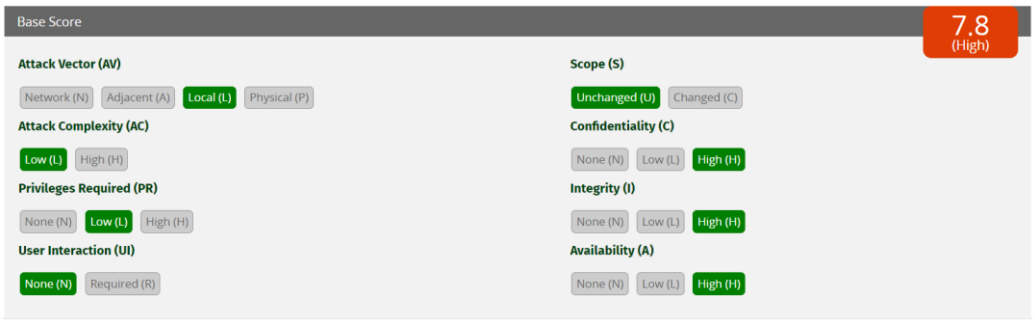
1. Pada hari Kamis, 6 Juni 2022, MITRE menerbitkan imbauan keamanan mengenai kerentanan *Use-After-Free Lead to Escalate Privilege* pada Linux Kernel 5.18.1.
2. Kerentanan ini dideskripsikan pada CVE-2022-32250 sebagai kerentanan yang memiliki dampak *High*.
3. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan ini, diharapkan pengguna dari produk terdampak ataupun pengguna pemerintah dan publik lainnya untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

Pendahuluan

MITRE merilis kerentanan baru yang dapat melakukan serangan *Use-After-Free Lead to Escalate Privilege* yang selanjutnya dideskripsikan pada CVE-2022-32250. Kerentanan ini memungkinkan pengguna untuk meningkatkan *privilege* menjadi *root*. Kerentanan ini dterjadi pada kernel linux 5.18.1 khususnya di net/netfilter/nf_tables_api.c.

Nilai Kerentanan

Berdasarkan CVSS 3.1, kerentanan ini memiliki nilai **7.8** yang dideskripsikan dalam CVE-2022-32250. Kerentanan ini dikategorikan sebagai *severity* **HIGH.**



Gambar 1. *Base Score* untuk Kerentanan CVE 2022-32250

Vector String (CVSS:3.1 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

Produk Terdampak

Produk yang terdampak oleh CVE 2022-32250 adalah Linux Kernel 5.18.1

Detail dan Dampak Kerentanan

Pada tanggal 6 Juni 2022, MITRE menerbitkan imbauan keamanan mengenai kerentanan *Use-After-Free Lead to Escalate Privilege* pada Linux Kernel 5.18.1 khususnya pada subsistem netfilter. Netfilter merupakan kerangka kerja di kernel linux untuk mengimplementasikan berbagai tugas terkait jaringan dengan penanganan yang ditentukan oleh pengguna. Netfilter menyediakan berbagai fungsi untuk penyaringan paket, terjemahan alamat jaringan dan terjemahan port, dan pencatatan paket. Subsistem netfilter yang rentan adalah nftables yang merupakan komponen netfilter yang memfilter atau merutekan ulang paket sesuai dengan aturan yang ditentukan oleh pengguna.

Use-After-Free merupakan kerentanan yang terjadi jika penunjuk heap terus digunakan setelah dibebaskan. Kerenan ini dapat menyebabkan eksekusi kode turunan. Dampak kerentanan ini pada kernel linux 5.18.1 yaitu memungkinkan pengguna lokal untuk melakukan *escalation privilege* menjadi root dikarenakan pemeriksaan NFT_STATEFUL_EXPR yang salah mengarah ke pengguna setelah terbebas dari memori. Kejadian tersebut Ketika nfset baru ditambahkan dengan perintah NFT_MSG_NESET. Saat memproses ekspresi pencarian dan dynset, potongan yang dibebaskan tetap berada di set->binding list karena pemeriksaan NFT_STATEFUL_EXPR yang salah. Hal inilah yang menyebabkan terjadinya kerentanan *Use-After-Free*.

Panduan Mitigasi

Untuk tindakan mitigasi dari CVE-2022–32250, MITRE menyarankan untuk menonaktifkan ruang nama pengguna dengan mengatur user.max_user_namespaces ke 0. Selain itu bagi pengguna yang menggunakan sistem operasi dengan berbasis kernel 5.18.1, dapat melakukan pemutakhiran versi kernel yang lebih baru.

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Jumat, 26 Agustus 2022

Ketentuan Penggunaan Dokumen

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

Referensi

[1] *"CVE-2022-32250"* https://access.redhat.com/security/cve/cve-2022-32250 (diakses 26 Agustus 2022)

[2] *"CVE-2022-32250"* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32250 (diakses 26 Agustus 2022).

[3] *"CVE-2022-32259 Detail"* https://nvd.nist.gov/vuln/detail/CVE-2022-32250#range-8269942 (diakses 26 Agustus 2022).

[4] *"Linux Kernel Exploit (CVE-2022-32250) With Mqueue"* https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/" (diakses 26 Agustus 2022).

[5] *"Kerentanan Use-After-Free"* https://tech-id.netlify.app/articles/id516150/index.html" (diakses 26 Agustus 2022).

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan
Pasar Minggu, Jakarta Selatan, 12550