7 Februari 2025

SECURITY ADVISORY
CVE-2024-43093

CVE-2024-43093 adalah kerentanan **eskalasi hak istimewa** pada Android Framework yang memungkinkan penyerang mengakses dan memodifikasi direktori sensitif seperti Android/data, Android/obb, dan Android/sandbox tanpa otorisasi. Android Framework adalah kumpulan API dan pustaka yang memungkinkan aplikasi berinteraksi dengan fitur inti sistem Android, seperti UI, sensor, jaringan, dan penyimpanan. Google mengonfirmasi bahwa kerentanan ini sedang dieksploitasi aktif, sehingga dapat menyebabkan kebocoran informasi serta peningkatan hak akses yang tidak sah pada perangkat yang terdampak.

Nilai/Tingkat

7.8
High

CWE
22

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Tipe kerentanan yang terjadi ketika suatu aplikasi tidak membatasi atau memvalidasi jalur *file* dengan benar, memungkinkan penyerang untuk mengakses *file* atau direktori di luar cakupan yang diizinkan.

Langkah Mitigasi

Segera perbarui perangkat Android ke patch keamanan terbaru November 2024, yang telah memperbaiki kerentanan ini. Informasi lebih detail dapat merujuk pada Android Security Bulletin November 2024. Hindari menginstal aplikasi dari sumber tidak tepercaya yang dapat mengeksploitasi kelemahan sistem. Selain itu, lakukan pemantauan rutin terhadap aktivitas perangkat untuk mendeteksi dan mencegah upaya eksploitasi yang mencurigakan.

Produk Terancam

Sistem operasi Android versi 12 hingga 14

Referensi Lanjutan, Solusi, dan Alat

- https://truefort.com/cve-2024-43093-android-flaw/
- https://thehackernews.com/2024/11/google-warns-of-actively-exploited-cve.html
- https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2024-43093
- https://www.cisa.gov/news-events/alerts/2024/11/07/cisa-adds-four-known-exploited-vulnerabilities-catalog

Informasi Imbauan Keamanan Lainnya di laman **Id-SIRTII/CC**

https://www.idsirtii.or.id/peringatan.html

Sumber Penulisan

- [Diakses 7 Februari 2025] https://nvd.nist.gov/vuln/detail/CVE-2024-43093
- [Diakses 7 Februari 2025] https://source.android.com/docs/security/bulletin/2024-11-01

Diterbitkan Oleh
Id-SIRTII/CC
Indonesia Security Incident Response team on Internet Infrastructure Coordination Center

Badan Siber dan Sandi Negara
(021) 788 33610
bantuan70@bssn.go.id
Jl. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550