Tidak Bisa Diperbaiki Lewat Update, Celah Keamanan “usbliter8” Intai Pengguna iPhone Lawas

Category: TEKNOLOGI
written by Redaksi | June 23, 2026

SEANTERONEWS.com – Sebuah perusahaan keamanan siber ofensif asal Barcelona, Spanyol, yang kerap mengembangkan perangkat lunak pengintai (spyware) dan alat peretasan untuk lembaga pemerintah, merilis laporan teknis mengenai adanya celah keamanan pada cip (chip) buatan Apple. Kerentanan ini berpeluang memudahkan para peretas profesional untuk membobol sistem keamanan perangkat iPhone model lawas.

Laporan mengenai celah keamanan yang dinamakan “usbliter8” tersebut dipublikasikan bersama sebuah bukti konsep

eksploitasi (proof of concept) oleh firma siber Paradigm Shift pada Jumat (19/6/2026) lalu.

Kerentanan perangkat keras ini memengaruhi jajaran ponsel iPhone yang ditenagai oleh cip Apple A12 Bionic dan A13 Bionic buatan tahun 2018 dan 2019, yang mencakup lini iPhone XS, iPhone XR, hingga keluarga besar iPhone 11.

Celah Permanen pada Benteng Pertama Boot ROM

Berdasarkan rilis teknisnya, kerentanan "usbliter8" ini menyerang bagian Boot ROM pada sistem pemrosesan iPhone. Boot ROM merupakan baris kode pemrograman pertama yang dijalankan oleh prosesor ketika perangkat pertama kali dinyalakan, sekaligus bertindak sebagai benteng pertahanan utama sistem operasi iOS terhadap upaya penyusupan luar.

Kerentanan pada bagian ini tergolong sangat krusial karena kode Boot ROM tertanam langsung secara permanen di dalam sirkuit silikon perangkat keras (immutable code) saat proses manufaktur di pabrik. Akibatnya, celah keamanan ini tidak akan pernah bisa ditambal atau diperbaiki melalui pembaruan sistem operasi (software patch) oleh pihak Apple.

"Karena kerentanan ini berada pada kode bawaan prosesor yang tidak dapat diubah, para pengguna perangkat terdampak harus menyadari bahwa beralih ke perangkat keras dengan cip yang lebih baru merupakan satu-satunya langkah mitigasi yang paling efektif," jelas pihak Paradigm Shift dalam keterangannya.

Butuh Akses Fisik dan Rantai Eksploitasi Tambahan

Kendati demikian, pengungkapan celah keamanan "usbliter8" ini tidak berarti bahwa seluruh perangkat iPhone lawas dapat diretas secara instan oleh siapa pun melalui internet. Untuk memanfaatkan celah ini, peretas harus memiliki akses fisik

langsung terhadap perangkat korban guna menghubungkan kabel data fisik.

Selain itu, menembus pertahanan awal Boot ROM hanyalah langkah pertama. Para peretas masih memerlukan rangkaian celah keamanan lain (vulnerability chaining) yang belum ditambal untuk dapat menembus enkripsi sistem dan mengakses data pribadi pengguna yang disimpan di dalam memori penyimpanan ponsel.

Bagi kalangan peneliti keamanan siber independen serta pembuat alat peretas komersial seperti Cellebrite dan Magnet Forensics yang biasa melayani kebutuhan forensik kepolisian informasi ini tergolong sangat berharga. Pengungkapan ini memfasilitasi riset untuk mengembangkan metode jailbreak (proses menembus batasan keamanan sistem operasi Apple) guna menemukan kerentanan sistem tingkat lanjut.

Paradigm Shift sendiri enggan memberikan tanggapan resmi ketika dimintai konfirmasi mengenai implikasi lanjut dari temuan “usbliter8” serta motif di balik pengumuman publik tersebut.[]