Screen Time & Parental Controls Bypass via "Find My" Remote Erase

Security Advisory & Technical Proof of Concept (PoC)

VULNERABILITY TYPE	Improper Access Control / Authorization Bypass (CWE-284)	**TARGET SYSTEM**	iOS / iPadOS (Screen Time & Find My Framework)
IMPACT ASSESSMENT	**High (Complete Local Restriction Bypass)**	**PREREQUISITES**	Physical or Device Access under Managed / Child Apple ID
AFFECTED FEATURE	Screen Time, Family Sharing, Parental Controls	**DATE SUBMITTED**	August 2026

1. EXECUTIVE SUMMARY

Summary: A fundamental security flaw exists in the authorization model between the native *Find My* app and *Screen Time / Parental Controls* restrictions. A restricted child account (or a device with a parent-enforced Screen Time passcode) can self-initiate a complete factory reset ("Erase This Device") directly from the local *Find My* interface without requiring the Screen Time passcode or parent authorization. Upon reboot, all enforced restrictions are permanently purged, granting unmonitored access.

2. ENVIRONMENT CONFIGURATION

The issue reproduces reliably under the following configuration:

- **Target Device:** iPhone or iPad running current iOS/iPadOS releases.
- **Account Setup:** Child Apple ID configured under Apple Family Sharing, managed by a Parent Apple ID.
- **Enforced Policies:** Active Screen Time restrictions (App Limits, Content & Privacy Restrictions, Allowed Apps).
- **Security Controls:** Screen Time Passcode set and maintained strictly by the Parent account.

3. PROOF OF CONCEPT (STEP-BY-STEP REPRODUCTION)

To demonstrate the vulnerability, execute the following steps directly on the restricted target device:

1. Launch the native `Find My` application on the restricted device.
2. Navigate to the **Devices** tab at the bottom navigation bar.
3. Locate and select the current local device (the child's own iPhone/iPad) from the device list.
4. Scroll to the bottom of the device management pane and tap **Erase This Device**.
5. Confirm the action. Note that the system prompts only for local confirmation without requesting the **Screen Time Passcode** or sending a real-time verification request to the Parent account.
6. Allow the device to undergo the full factory wipe procedure.
7. Upon restart, proceed through the standard iOS Setup Assistant as an unmanaged device.

4. BEHAVIOR ANALYSIS

EXPECTED SECURITY BEHAVIOR	ACTUAL OBSERVED VULNERABILITY
Enforced Authorization Guard: The system should identify that the device is subject to parental management or Screen Time passcode protection, blocking the factory erase function unless authenticated by the parent or authorized via Screen Time passcode.	**Unchecked Self-Erase Execution:** The *Find My* service executes the local factory reset command immediately. Screen Time locks, app bans, web filters, and daily limits are completely wiped without parental notification or intervention.

5. SECURITY & PRIVACY IMPACT

- **Complete Control Subversion:** Enables non-privileged users (children) to unilaterally dismantle security and privacy controls established by system administrators (parents).
- **Zero Audit Trail / Notification:** The factory reset bypass occurs locally without requiring explicit approval from the primary Family Organizer account.
- **Access Control Logic Flaw:** Represents a failure to enforce authorization boundaries between distinct iOS subsystems (*Find My* daemon vs. *Screen Time* policy enforcement daemon).

6. SUGGESTED REMEDIATION

PROPOSED FIX / RECOMMENDATION

1. **Passcode Challenge Integration:** Intercept the "Erase This Device" workflow within the *Find My* app to prompt for the Screen Time passcode whenever active restrictions exist.
2. **Family Organizer Authorization:** For accounts managed under Family Sharing as a Child Account, require approval from the Family Organizer (via *Ask to Buy / Approve* prompt or Family ID authentication) prior to initiating a local erase.