FRP bypass vulnerability

+1 Hotlists (1) Mark as Duplicate

Comments (39) Dependencies Duplicates (0) Blocking (0) Resources (15)

WAI Bug P2 + Add Hotlist

STATUS UPDATE No update yet.

DESCRIPTION bu...@google.com created issue on behalf of Derek Morris #1 Jul 10, 2024 09:53AM

Report description

FRP bypass vulnerability

Bug location

Where do you want to report your vulnerability?

Android & Devices VRP – Report security issues affecting Pixel, Google Nest, Pixel Watch, and Fitbit devices and their latest operating systems. See program rules

The problem

Please describe the technical details of the vulnerability

Google pixel phone has a vulnerability allowing a person to bypass the FRP lock, even with the phones bootloader locked and usb debugging disabled using the latest updated firmware to gain access.

Please briefly explain who can exploit the vulnerability, and what they gain when doing so

Anyone who has access to the device and basic knowledge of using a computer can exploit the vulnerability, attackers can gain unauthorized access to the device and potentially steal sensitive information stored on it, such as personal data, login credentials, and financial information. An attacker could also use the device for wide scale criminal activity without being traced.

The cause

Please specify the steps to reproduce the issue, including sample code where appropriate. Please be as detailed as possible.

1. google pixel 6 with android 14 on June (Spl) with a locked bootloader, usb debugging settings disabled, google account and a user lock tied to the device.
2. using a computer download android platform tools latest release, pixel flasher tool latest release, and android 15 beta 3.1 OTA image latest release.
3. open pixel flasher tool and place the platform tools folder in the required directory.
4. place the android 15 beta OTA image file in the device image directory in the tool.
5. turn on the google pixel 6, and boot into recovery using volume button down and power button held at the same time,(you should be in bootloader menu) scroll through menu and select recovery and press power button to reboot, you should now be in recovery menu.
6. scroll down to factory reset wipe device option to reset device, select yes, when process is finished select reboot to system.
7. you should now see the lock symbol in upper left corner of the pixel 6 screen with the welcome message, proceed with the setup process, add google account, set user lock pin, go through the rest of the setup process to make sure google account is added to the device.
8. go into the settings menu and make sure that OEM unlocking menu is disabled(do not allow the bootloader to be unlocked), this way we know that the device protection feature is active(FRP).
9. go into settings menu and make sure to check if developer option menu showing, if it is go into developer menu and make sure usb debugging is disabled, and then disable developer options.
10. reboot pixel 6 again and you should see welcome message again and the lock symbol at the upper left corner of pixel screen, continue the setup process on the pixel as if you did not know any of the account information linked to the device, you should come to the lock screen asking for a pin, and google account information.
11. reboot the pixel into recovery menu again and go back into the pixel flasher tool.
12. attach a usb type-c cable capable of transfering data(not just a charger cable) to the computer and the phone.
13. on the pixel device in recovery menu select apply update from adb, you should see the message on the pixel waiting for the sideload.
14. back in the pixel flasher tool, click on the scan button so it will detect the pixel in sideload mode, you will see it under the heading adb connected devices.
15. in the flasher tool where you loaded the android 15 beta OTA image file you want to click on the process button and you will see it loading the information into the console in the tool, you will also see the bootloader show up in the console right below the directory where the image file is that you loaded.
16. click on the bootloader information in that console and you will see it turn blue and directly below that you should now see the button with the heading that says flash pixel phone in bold black lettering and in the upper menu you will notice a check box enabled with the heading full ota flash, now click on the button that says flash pixel phone and you will see all the flash information in the main console.
17. when it finishes unplug the device and boot it into the system and you should now be at welcome screen without a lock symbol in the upper corner of the pixel screen, proceed to setup the device and you will come to a screen that says this device is enrolled in the beta program, at this point you can now go into settings, enable developer menu, unlock the bootloader, and flas whatever custom rom, factory rom, or ota rom that you choose and setup your google account information also.

Expanded access is turned on for this component. Assignees, verifiers and collaborators can edit issues in this component, and CC'd users can comment on them. Learn more

Specify the build fingerprint from the device used to reproduce the issue. The issue should reproduce on a recent build (within the last 30 days).

google/oriole/oriole:14/AP2A.240605.024/11860263:user/release-keys

Does anyone else know about this vulnerability?

No, this vulnerability is private

Do you plan to disclose this bug publicly?

No

How would you like to be publicly acknowledged for your report?