

main

...

Panasonic-WV-S2231L / README.md



cecada Initial commit

History

1 contributor

27 lines (13 sloc) | 1.23 KB

...

## CVE-2020-35768

Details to come.

## CVE-2020-29193

UART can easily be obtained via the detachable PCB which houses the Sony Xarina ARM chip (just to the left, and slightly above the 'S' as you read the word Sony). Upon UART access the following findings were made:

1. No password U-Boot, allows the ability to set bootargs, up/download data via TFTP, boot random images, write to flash, etc.
2. System boots right into a root shell with no authentication needed. This allows the ability to launch telnetd and nc are present for remote access. TFTP can be used to up/download data.
3. Root (which is accessible via telnet) has an insecure static/hard coded password (more detials to come).

With initial physical access, an attacker could easily exploit these vulnerabilities to obtain remote access, monitor data, disable security, or any number of other things.

## CVE-2020-29194

Sending a malformed HTTP POST request to the camera will cause a denial of service of the admin control panel which will require a physical reset to restore administrative control.

More details to come.