# Errata Slip #3

## Proceedings of the 28th USENIX Security Symposium

For the paper "FIRM-AFL: High-Throughput Greybox Fuzzing of IoT Firmware via Augmented Process Emulation" by Yaowen Zheng, Ali Davanian, Heng Yin, Chengyu Song, Hongsong Zhu and Limin Sun, (Thursday session, "IoT Security," pp. 1099–1114 of the Proceedings) the authors have provided the following correction. In the original version, the 5th, 6th, 7th and 9th subfigure in Figure 7 and corresponding results in Table 6 are incorrect. The corrected figure and table are as below. We can see that the throughput of FIRM-AFL is on average 9.2 times (8.2 times in original version) higher than system-mode emulation based fuzzing.

| Exploit ID | Vendor | Model | Version | Device | Program | Full-System<br>Time to crash | FIRM-AFL<br>Time to crash |
|---|---|---|---|---|---|---|---|
| CVE-2018-19242 | Trendnet | TEW-632BRP | 1.010B32 | Router | httpd | 3h18min | 21min |
| CVE-2013-0230 | Trendnet | TEW-632BRP | 1.010B32 | Router | miniupnpd | >24h | 9h16min |
| CVE-2018-19241 | Trendnet | TV-IP110WN | V.1.2.2 | Camera | video.cgi | 19h13min | 4h55min |
| CVE-2018-19240 | Trendnet | TV-IP110WN | V.1.2.2 | Camera | network.cgi | 2h43min | 15min |
| CVE-2017-3193 | DLink | DIR-850L | 1.03 | Router | hnap | 21h3min | 2h54min |
| CVE-2017-13772 | TPLink | WR940N | V4 | Router | httpd | >24h | >24h |
| EDB-ID-24926 | DLink | DIR-815 | 1.01 | Router | hedwig.cgi | 16h38min | 1h22min |
| EDB-ID-38720 | DLink | DIR-817LW | 1.00B05 | Router | hnap | 4h26min | 1h29min |
| EDB-ID-38718 | DLink | DIR-825 | 2.02 | Router | httpd | >24h | 6h4min |
| CVE-2016-1558 | DLink | DAP-2695 | 1.11.RC044 | Router | httpd | 16h24min | 2h32min |
| CVE-2018-10749 | DLink | DSL-3782 | 1.01 | Router | tcapi | 247s | 20s |
| CVE-2018-10748 | DLink | DSL-3782 | 1.01 | Router | tcapi | 252s | 22s |
| CVE-2018-10747 | DLink | DSL-3782 | 1.01 | Router | tcapi | 249s | 20s |
| CVE-2018-10745 | DLink | DSL-3782 | 1.01 | Router | tcapi | 236s | 25s |
| CVE-2018-8941 | DLink | DSL-3782 | 1.01 | Router | tcapi | 281s | 24s |

Table 6: 1-day exploits

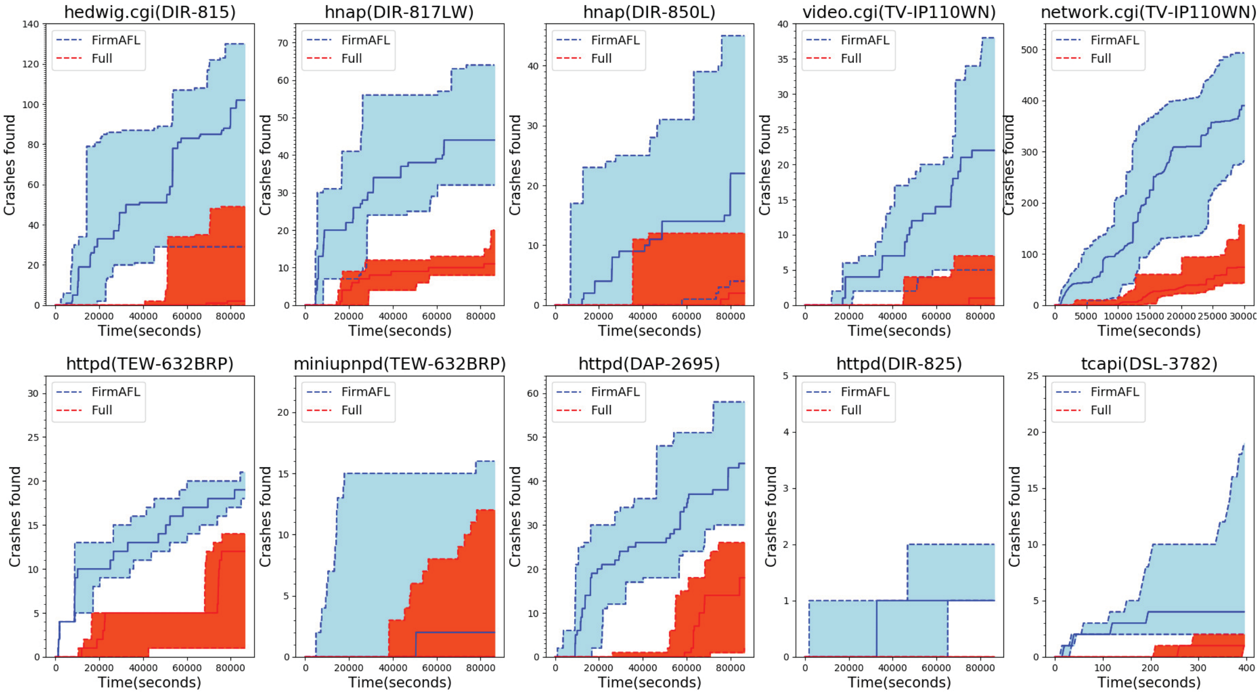

Figure 7: Crashes found over time