CVE-2017-6956

描述：On the Broadcom Wi-Fi HardMAC SoC with fbt firmware, a stack buffer overflow occurs when handling an 802.11r (FT) authentication response, leading to remote code execution via a crafted access point that sends a long R0KH-ID field in a Fast BSS Transition Information Element (FT-IE).

软件：Broadcom Wi-Fi HardMAC SoC

源码：src/common/wpa\_common.c

出现位置： 1170-1182行

关键源码：

if (ssid\_len > SSID\_MAX\_LEN || r0kh\_id\_len > FT\_R0KH\_ID\_MAX\_LEN)

return -1;

pos = buf;

\*pos++ = ssid\_len;

os\_memcpy(pos, ssid, ssid\_len);

pos += ssid\_len;

os\_memcpy(pos, mdid, MOBILITY\_DOMAIN\_ID\_LEN);

pos += MOBILITY\_DOMAIN\_ID\_LEN;

\*pos++ = r0kh\_id\_len;

os\_memcpy(pos, r0kh\_id, r0kh\_id\_len);

pos += r0kh\_id\_len;

os\_memcpy(pos, s0kh\_id, ETH\_ALEN);

pos += ETH\_ALEN;