



```
10     QSPI_Read_Product_Headers((struct_configuration_script_ptr *)&configuration_script, product_img_offsets);
10 }
106 while ( BYTE1(configuration_script) != 1 );
106 WDOG_feed_ff();
107 if ( check_current_fw_addr_and_update_addr(product_img_offsets) )// differing offsets mean we have an update, enter
108 {
109     if ( !SECUREBOOT_check_and_validate(
110         product_img_offsets[1],
111         (FW_ImageHeader *)&dword_2003C950,
112         (int)product_img_offsets,
113         (struct_configuration_script_ptr *)&configuration_script) )// / returns 1 if secure boot is not enabled
114     {
115         QSPI_process_product_update((struct_configuration_script_ptr *)&configuration_script, product_img_offsets); // re
116         WDOG_Pet_1c34();
117     }
118 } // no update path
119 // this returns 0 from [8] offset check
120 //    if ( !( *qspi_data_value_ptr )[8] )
121 //        return 0;
122 else if ( !SECUREBOOT_check_and_validate(
123     product_img_offsets[0],
124     (FW_ImageHeader *)&dword_2003C950,
125     (int)product_img_offsets,
126     (struct_configuration_script_ptr *)&configuration_script) )// returns 1 if secure boot is not enabled
127 {
128     WDOG_Pet_1c34(); // we hit this
129 }
130 SECUREBOOT_CHECK_key_revocation(dword_2003C950);
131 sub_A6E((struct_configuration_script_ptr *)&configuration_script, product_img_offsets);
132 WDOG_feed_ff();
133 if ( !SECUREBOOT_CHECK_setup_QSPIC_CTR_195C(
134     (struct_configuration_script_ptr *)&configuration_script,
135     product_img_offsets) )
136     WDOG_Pet_1c34();
137 OTPC_standby();
138 Cache_setup_qspi_cache(dword_2003C950, product_img_offsets);
139 write_to_sysram(dword_2003C950, product_img_offsets);
140 return RESET_to_REMAP_ADR_val(2u); // SW Reset to QSPI Flash
141 }
```

CVE-2024-25076



```
10     QSPI_Read_Product_Headers((struct_configuration_script_ptr *)&configuration_script, product_img_offsets);
11 }
12 while ( BYTE1(configuration_script) != 1 );
13 WDOG_feed_ff();
14 if ( check_current_fw_addr_and_update_addr(product_img_offsets,
15 {
16     if ( !SECUREBOOT_check_and_validate(
17         product_img_offsets[1],
18         (FW_ImageHeader *)&dword_2003C950,
19         (int)product_img_offsets,
20         (struct_configuration_script_ptr *)&configuration_script) )// / returns 1 if secure boot is not enabled
21     {
22         QSPI_process_product_update((struct_configuration_script_ptr *)&configuration_script, product_img_offsets); // re
23         WDOG_Pet_1c34();
24     }
25 }
26     // no update path
27     // this returns 0 from [8] offset check
28     // if ( !( *qspi_data_value_ptr )[8] )
29     //     return 0;
30
31 else if ( !SECUREBOOT_check_and_validate(
32     product_img_offsets[0],
33     (FW_ImageHeader *)&dword_2003C950,
34     (int)product_img_offsets,
35     (struct_configuration_script_ptr *)&configuration_script) )// returns 1 if secure boot is not enabled
36 {
37     WDOG_Pet_1c34(); // we hit this
38 }
39 SECUREBOOT_CHECK_key_revocation(dword_2003C950);
40 sub_A6E((struct_configuration_script_ptr *)&configuration_script, product_img_offsets);
41 WDOG_feed_ff();
42 if ( !SECUREBOOT_CHECK_setup_QSPI_CTR_195C(
43     (struct_configuration_script_ptr *)&configuration_script,
44     product_img_offsets) )
45     WDOG_Pet_1c34();
46 OTPC_standby();
47 Cache_setup_qspi_cache(dword_2003C950, product_img_offsets);
48 write_to_sysram(dword_2003C950, product_img_offsets);
49 return RESET_to_REMAP_ADR_val(2u); // SW Reset to QSPI Flash
50 }
```

CVE-2024-25076

ENCRYPTION

Key Indexes

- Index into OTP for encryption engine

Nonce

- User defined Nonce
- Avoid IV reuse

AES-CTR mode enables fast/arbitrary block decryption

AES-CTR provides no auth (malleable)

