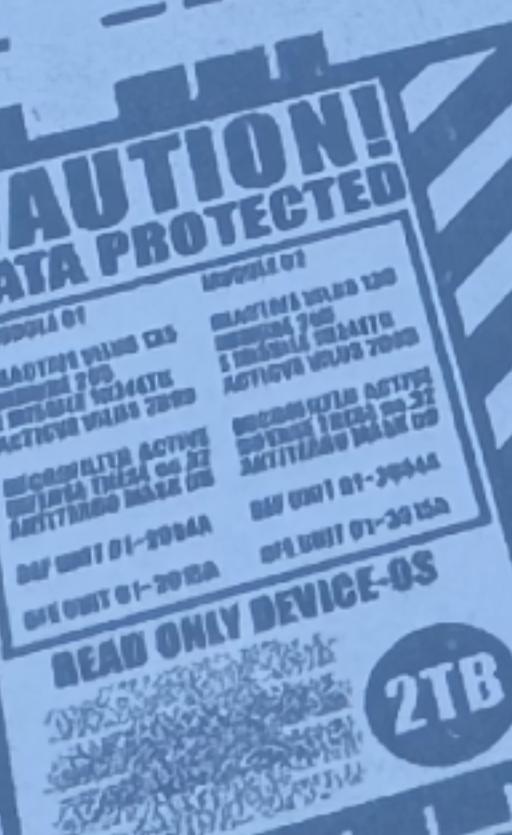


廣東工業品化學品工檢業查限公司



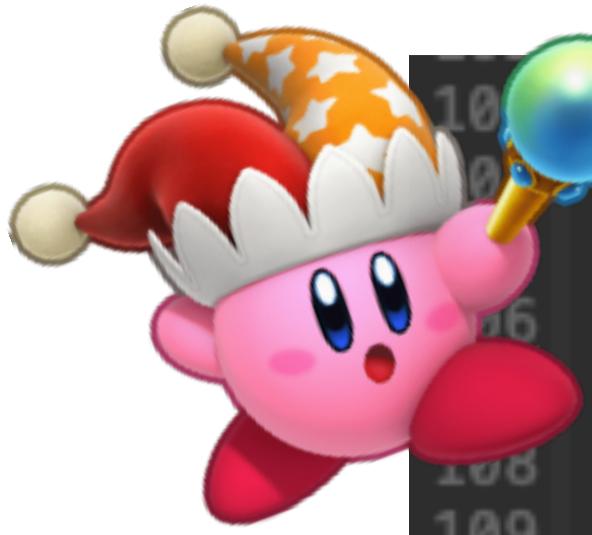
R258

GORNY.TOOLS

READ ONLY DEVICE

2TR

20
km/h



```
100     QSPI_Read_Product_Headers((struct_configuration_script_ptr *)&configuration_script, product_img_offsets);
101 }
102 while ( BYTE1(configuration_script) != 1 );
103 WDOG_feed_ff();
104 if ( check_current_fw_addr_and_update_addr(product_img_offsets) )// differing offsets mean we have an update, enter
105 {
106     if ( !SECUREBOOT_check_and_validate(
107         product_img_offsets[1],
108         (FW_ImageHeader *)&dword_2003C950,
109         (int)product_img_offsets,
110         (struct_configuration_script_ptr *)&configuration_script) )// / returns 1 if secure boot is not enabled
111     {
112         QSPI_process_product_update((struct_configuration_script_ptr *)&configuration_script, product_img_offsets); // re
113         WDOG_Pet_1c34();
114     }
115     // no update path
116     // this returns 0 from [8] offset check
117     //   if ( !( *qspi_data_value_ptr )[8] )
118     //       return 0;
119
120     else if ( !SECUREBOOT_check_and_validate(
121         product_img_offsets[0],
122         (FW_ImageHeader *)&dword_2003C950,
123         (int)product_img_offsets,
124         (struct_configuration_script_ptr *)&configuration_script) )// returns 1 if secure boot is not enabled
125     {
126         WDOG_Pet_1c34(); // we hit this
127     }
128     SECUREBOOT_CHECK_key_revocation(dword_2003C950);
129     sub_A6E((struct_configuration_script_ptr *)&configuration_script, product_img_offsets);
130     WDOG_feed_ff();
131     if ( !SECUREBOOT_CHECK_setup_QSPIC_CTR_195C(
132         (struct_configuration_script_ptr *)&configuration_script,
133         product_img_offsets) )
134         WDOG_Pet_1c34();
135     OTPC_standby();
136     Cache_setup_qspi_cache(dword_2003C950, product_img_offsets);
137     write_to_sysram(dword_2003C950, product_img_offsets);
138     return RESET_to_REMAP_ADR_val(2u); // SW Reset to QSPI Flash
139
140
141 }
```

CVE-2024-25076



CVE-2024-25076

```
100     QSPI_Read_Product_Headers((struct_configuration_script_ptr *)&configuration_script, product_img_offsets);
101 }
102 while ( BYTE1(configuration_script) != 1 );
103 WDOG_feed_ff();
104 if ( check_current_fw_addr_and_update_addr(product_img_offsetse
105 {
106     if ( !SECUREBOOT_check_and_validate(
107         product_img_offsets[1],
108         (FW_ImageHeader *)&dword_2003C950,
109         (int)product_img_offsets,
110         (struct_configuration_script_ptr *)&configuration_script )/// / returns 1 if secure boot is not enabled
111     {
112         QSPI_process_product_update((struct_configuration_script_ptr *)&configuration_script, product_img_offsets); // re
113         WDOG_Pet_1c34();
114     }
115 }
116 }
117 }
118 }
119 }
120 }
121 }
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_QSPI_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 }
```

ENCRYPTION

Key Indexes

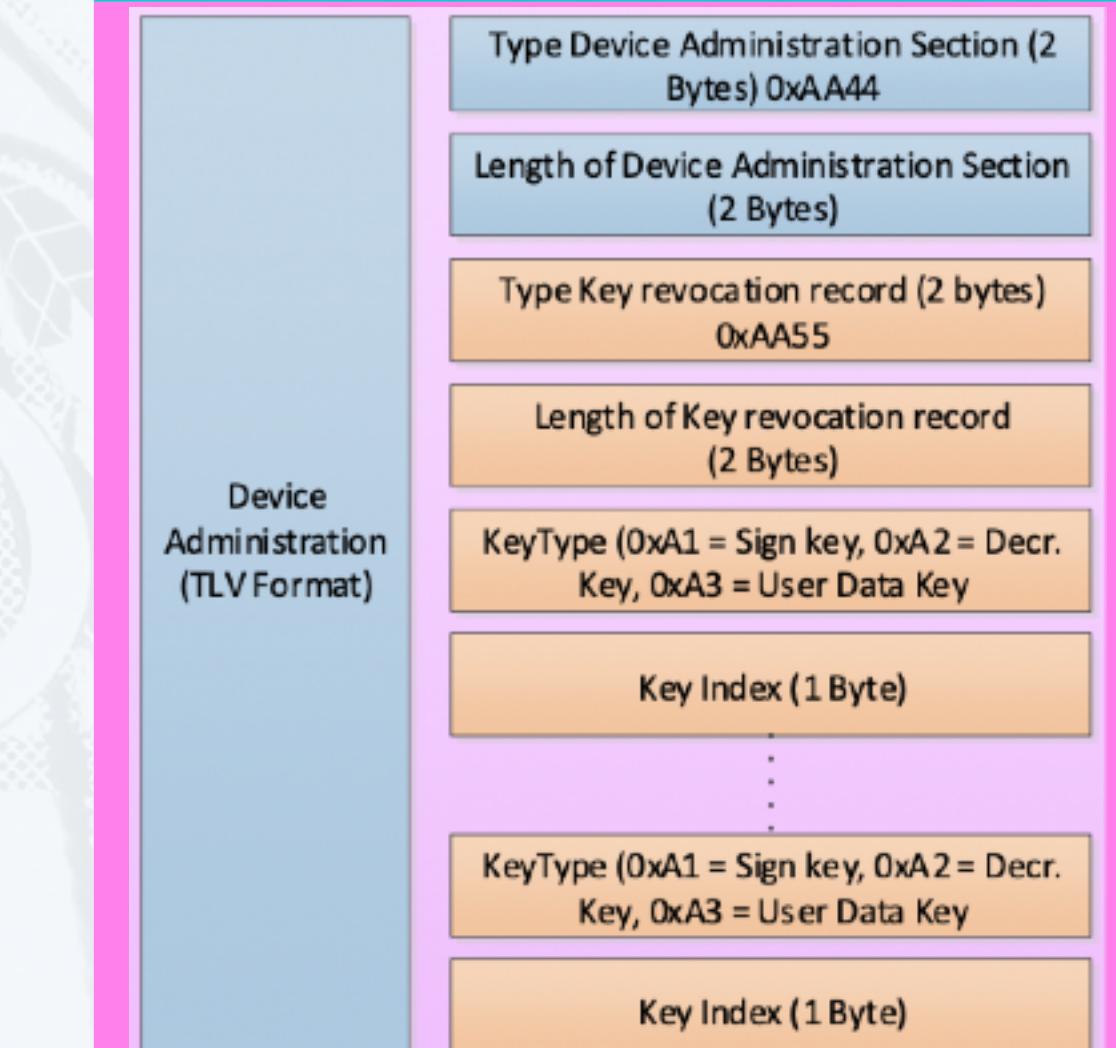
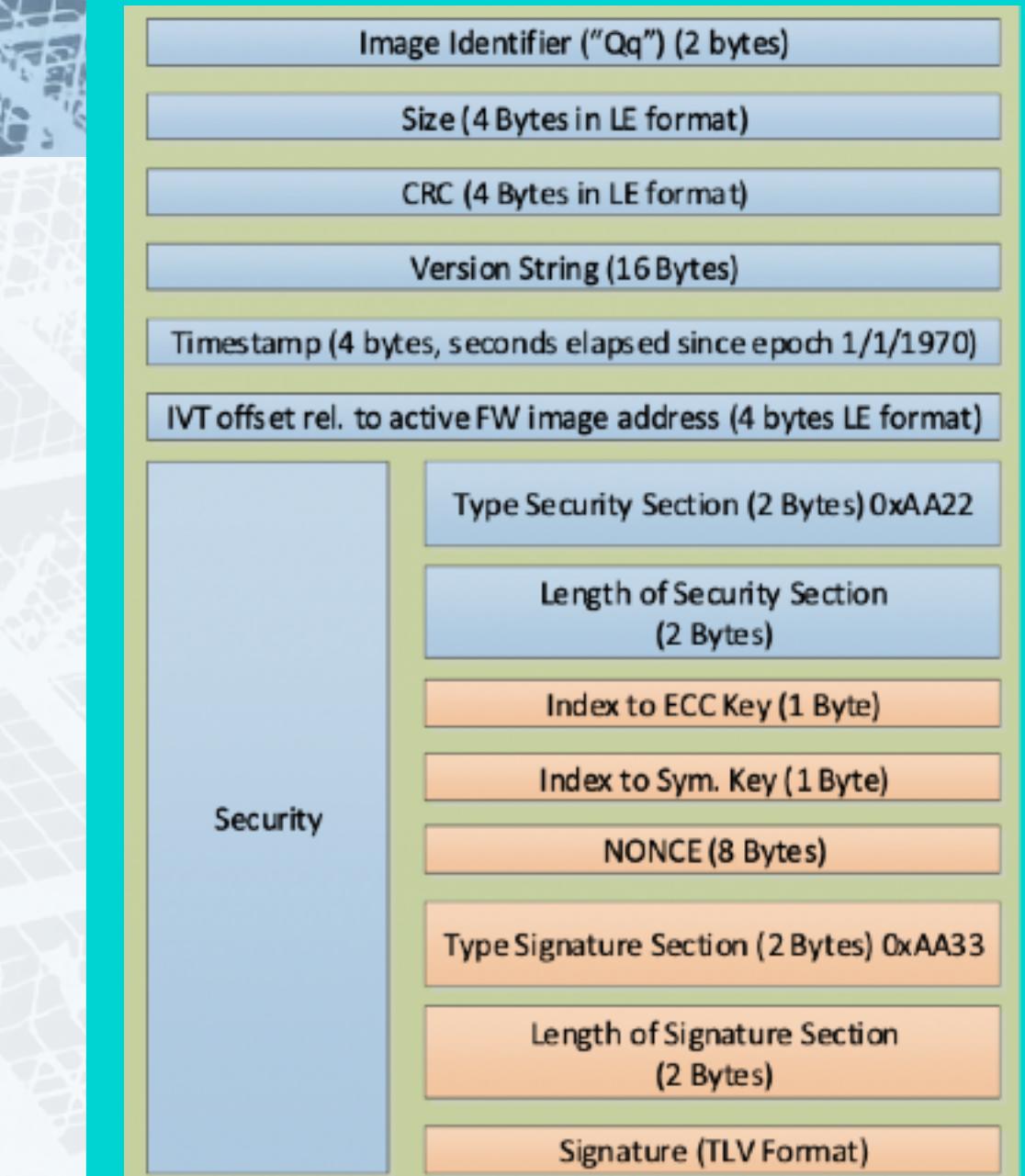
- Index into OTP for encryption engine

Nonce

- User defined Nonce
- Avoid IV reuse

AES-CTR mode enables fast/arbitrary block decryption

AES-CTR provides no auth (malleable)



SIGNED

ENCRYPTED