WinMin / **Disclosure of vulnerabilities in Vigor2960 and Vigor3900.md**

Disclosure of vulnerabilities in Vigor2960 and Vigor3900

Disclosure of vulnerabilities in Vigor2960 and Vigor3900.md

Version

Vigor2960 fw1.5.1.1RC3 (r8167) Vigor3900 fw1.5.1.1beta_r8167

Vulnerability details

There are some command injection vulnerabilities in the mainfunction.cgi file. The details are as follows:

1. in downlaod_ovpn function

The parameters from http_input are written directly to the buf of s without filtering, followed by system, which can causecommand injection

2. in doOpenVpn function

The value of "option" is from "http_input" and later concatenated and used by "system" without any special characters sanitizing, causing command injection

3. int dumpSyslog_func

The value of "option" is from "http_input", and single quote character allowed. So, since it is user-controllable, when user input closes the single quote, a command injection is done.

4. in get_subconfig_func

"rtick" is from "http_input", and further passed to "sub_F2D8". In "sub_F2D8", "rtick" is concatenated to "/tmp/ipv6_neigh_", then passed to "system", causing command injection.

5. in set_ap_map_config_func
The value of "option" is from "http_input",and will be spliced with "/sbin/ipsec_new_cer" , may cause command execution

6. in delete_wlan_profile_func

The value of "profile_number " is from "http_input" and will be spliced with "uci delete apm_wlan_profile.profile" , may cause command execution

7. in ruequest_certificate_func

The value of "option" will be spliced with "/sbin/ipsec_new_cer" , may cause command execution

8. in doGRETunnel_func

The table value will be spliced with "/etc/init.d/gretunnel disconnect_from_web '%s' 1>/dev/null 2>&1" , may cause command execution

Discoverer

swing@chaitin
Cossack9989@NJUPT

Final

Thanks for draytek's instant response!

Timeline

2020.05.29 report these vulnerabilities
2020.06.01 vendor reply
2020.06.04 vendor fix these vulnerabilities
2020.06.17 vendor released new firmware