NVD DB Update

CVE-2021-35395 - Score: 9.8

Components:

realtek realtek jungle sdk *

Description:

Realtek Jungle SDK version v2.x up to v3.4.14B provides an HTTP web server exposing a management interface that can be used to configure the access point. Two versions of this management interface exists: one based on Go-Ahead named webs and another based on Boa named boa. Both of them are affected by these vulnerabilities. Specifically, these binaries are vulnerable to the following issues: - stack buffer overflow in formRebootCheck due to unsafe copy of submit-url parameter - stack buffer overflow in formWsc due to unsafe copy of submit-url parameter - stack buffer overflow in formWlanMultipleAP due to unsafe copy of submit-url parameter - stack buffer overflow in formWlSiteSurvey due to unsafe copy of ifname parameter - stack buffer overflow in formStaticDHCP due to unsafe copy of hostname parameter - stack buffer overflow in formWsc due to unsafe copy of 'peerPin' parameter - arbitrary command execution in formSysCmd via the sysCmd parameter - arbitrary command injection in formWsc via the 'peerPin' parameter Exploitability of identified issues will differ based on what the end vendor/ manufacturer did with the Realtek SDK webserver. Some vendors use it as-is, others add their own authentication implementation, some kept all the features from the server, some remove some of them, some inserted their own set of features. However, given that Realtek SDK implementation is full of insecure calls and that developers tends to re-use those examples in their custom code, any binary based on Realtek SDK webserver will probably contains its own set of issues on top of the Realtek ones (if kept). Successful exploitation of these issues allows remote attackers to gain arbitrary code execution on the device.

Main problems: