

New issue

[Jump to bottom](#)

# HTTP Server File upload leads to Code Execution #52

🔓 Open feric opened this issue on Jun 19 · 2 comments

Labels bug Hiby R3 Pro Series Security

feric commented on Jun 19

Through the File upload feature, it is possible to replace .sh files in the device with malicious content, leading to execute os commands on the device as root user.

The vulnerability is described in the below URL:

<https://github.com/feric/Findings/tree/main/Hiby/Web%20Server/File%20uploading>

This finding was found in firmware 1.5; however, is still present in the latest 1.7 firmware for the R3 Pro Saber.

 vext01 added bug Hiby R3 Pro Series Security labels on Jun 28

vext01 commented on Jun 28

Owner



vext01 commented on Jun 28

Owner

Are you able to start sshd?

Assignees

No one assigned

Labels

bug Hiby R3 Pro Series Security

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

