

[New issue](#)[Jump to bottom](#)

XSS through Emergency Alert #28

[Open](#)

Securitybits-io opened this issue on Feb 16 · 0 comments

Labels

enhancement

Milestone

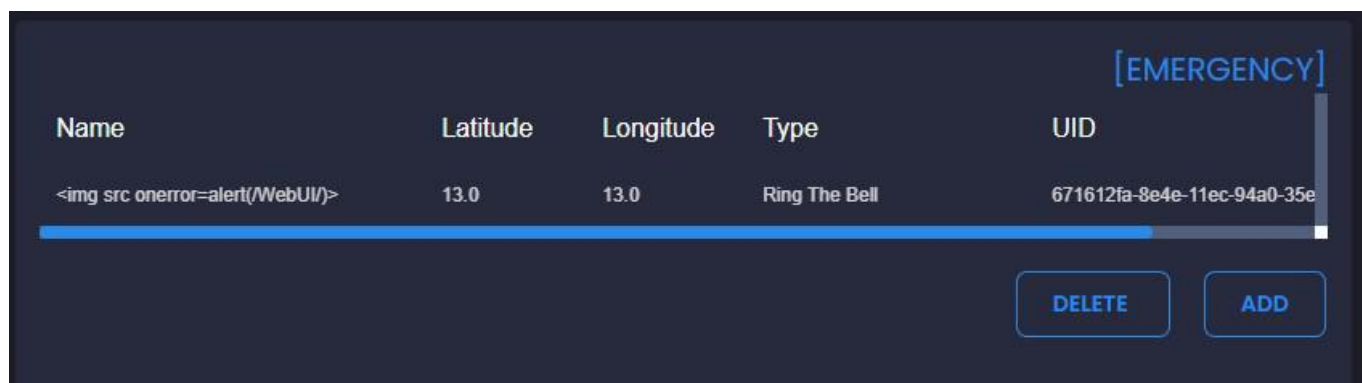
2.4

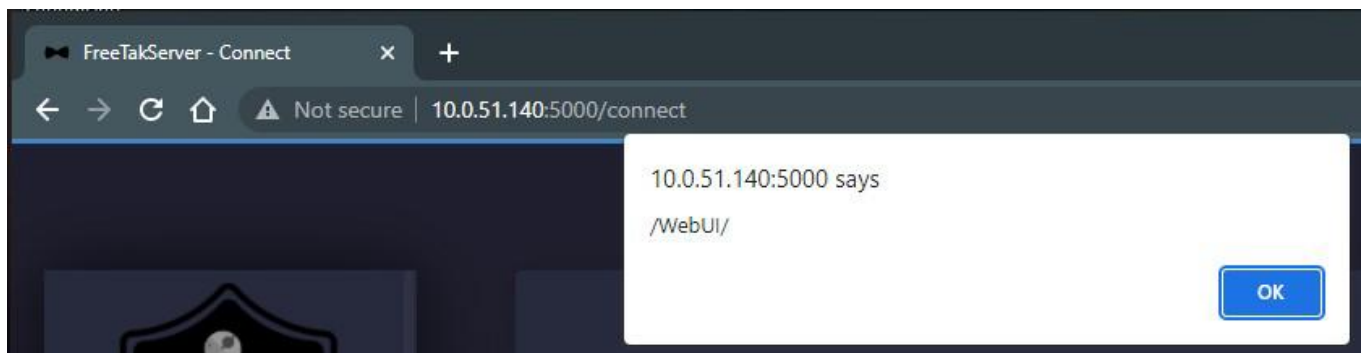
Securitybits-io commented on Feb 16

In the FreeTAKServer-UI there is a function to create and view Emergency Alerts that are originating from either the End User Device or from the UI itself. Both Avenues are susceptible to a Stored Cross Site scripting vulnerability in the Callsign parameter.

Web Interface

In the case of a XSS in the WebUI it is as simple as having a callsign with the payload of `` which will trigger the Emergency function and display the emergency in the WebUI.

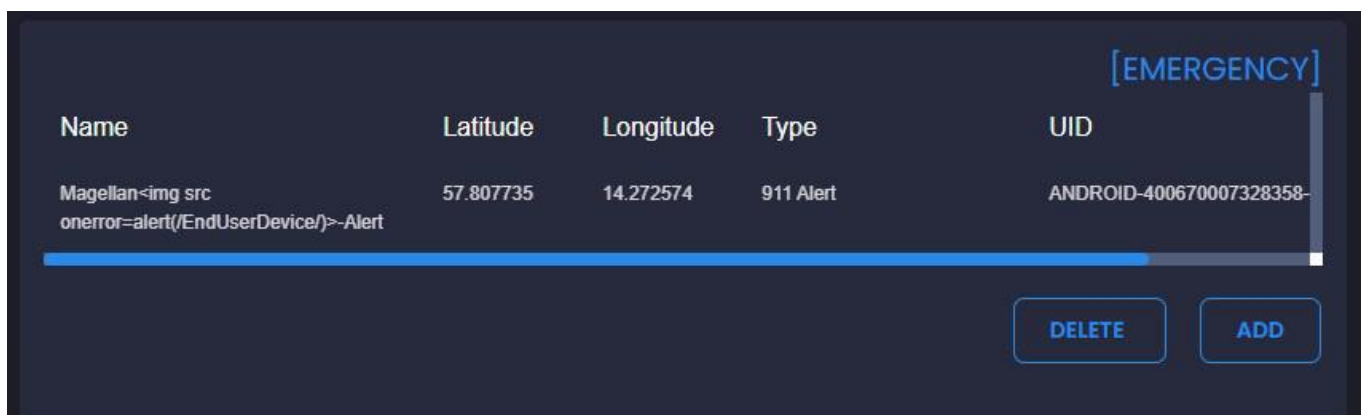
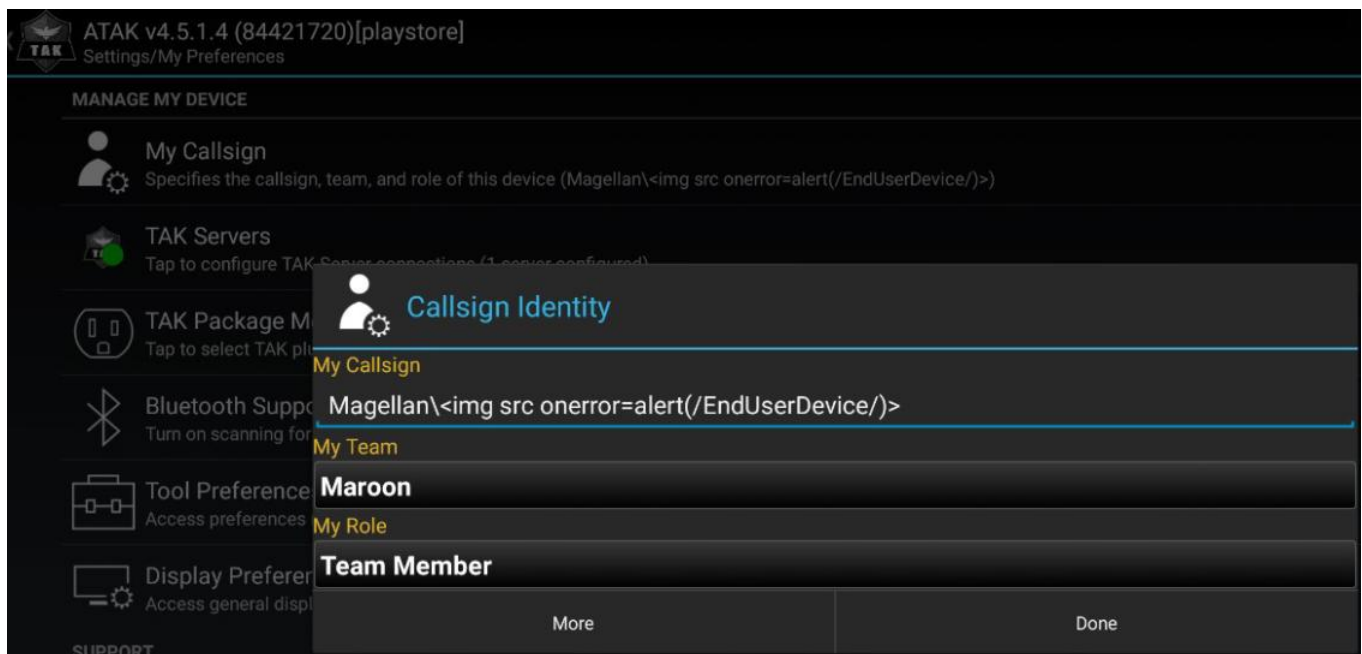


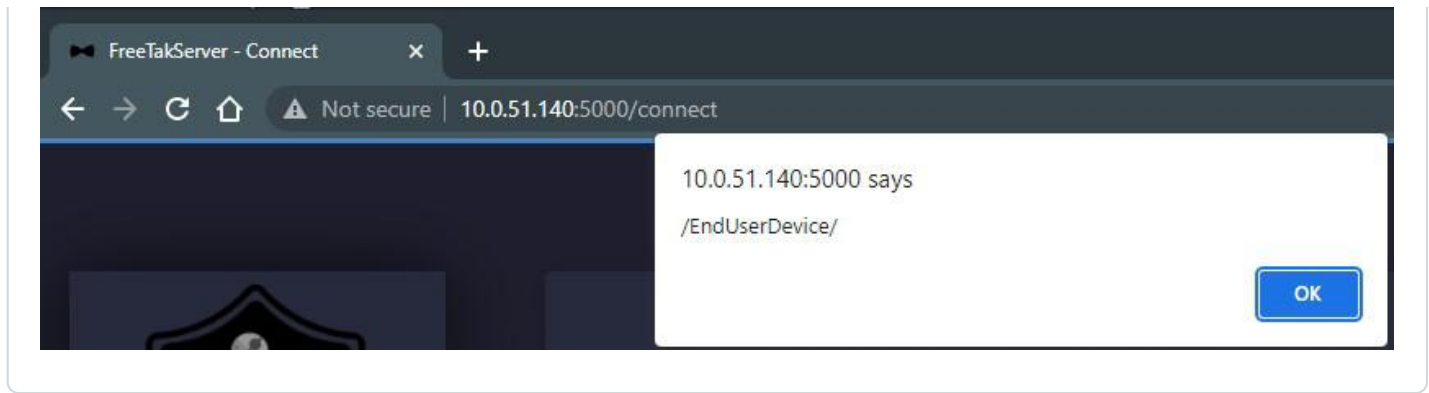




End User Device

What's more interesting of a scenario is that it is possible to push Emergencies from any of the EUDs, these can range from a 911, TIC (Troops in Contact) or similar.

This can be chained together with the API keys leakage in the response in order to obtain a server RestAPI key for further exploitation, which can take a normal user in the field to a Web Server admin





  brothercorvo added the **enhancement** label on Sep 6

  brothercorvo added this to the **2.4** milestone on Sep 14

Assignees

No one assigned

Labels

enhancement

Projects

None yet

Milestone

2.4

Development

No branches or pull requests

2 participants

