

payload payload 0.5.0

### Description:

pyLoad is a free and open-source Download Manager. The folder './pyload/scripts' has scripts which are run when certain actions are completed, for e.g. a download is finished. By downloading a executable file to a folder in /scripts and performing the respective action, remote code execution can be achieved in versions prior to 0.5.0b3.dev87. A file can be downloaded to such a folder by changing the download folder to a folder in '/scripts' path and using the '/flashgot' API to download the file. This vulnerability allows an attacker with access to change the settings on a pyload server to execute arbitrary code and completely compromise the system. Version 0.5.0b3.dev87 fixes this issue.

### Main problems:

78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')"