

Vulnerability : Remote Code Execution Vulnerability
Authentication : Low Privileged Access to Web Console Required
Exploitability : Easy
Access Vector: Network
CIA: Affected Completely

Steps to Reproduce:

- 1) Create a low privileged account having access to the web console
- 2) Login via the account created and navigate to File Management -> File Manager Console
- 3) Select any folder and click on compress .
- 4) An option will be presented to provide name for the new compressed file
- 5) Give any name in below format
Filename`command`.tar ex: test`id`.tar
- 6) This will lead to a new file being created with name testuid=1001(test) as seen in below snapshot.

The screenshot displays the CWP Control Web Panel interface. On the left, a sidebar shows a file tree with folders like .cache, .conf, .config, .dbus, .mozilla, and .pki. The main area shows the 'tmp' directory with a table of files. The table has columns for Name, Perm, Owner, Group, Size, and Date. A file named 'testuid=1001(test)' is listed with permissions 0644, owned by 'test', with a size of 644 bytes, and created on 23/02/20 at 06:35.

Name	Perm	Owner	Group	Size	Date
session	0751	test	test		23/02/20 06:22
testuid=1001(test)	0644	test	test	644 bytes	23/02/20 06:35