[Deluge] #3460: XSS via malicious .torrent file

33 views

Deluge Mar 1, 2021, 3:23:05 PM

to delug...@googlegroups.com

#3460: XSS via malicious .torrent file
----------+----------
Reporter: jasperla | Type: bug
Status: new | Priority: major
Milestone: needs verified | Component: Web UI
Version: develop | Keywords:
----------+----------
The Deluge web ui is vulnerable to XSS through a crafted torrent file.

As the data from torrent files is not properly sanitised it's interpreted directly as HTML. As such someone who supplies the user with a malicious torrent can execute arbitrary Javascript code in the context of the user's browser session. It should be noted that the Tornado webserver is not configured to send any `Content-Security-Policy` headers which can help to mitigate some of the impact. Due to this omission, the attacker can download/upload arbitrary data from/to remote endpoints.

It should be noted there is some basic filtering such that a `<script>` doesn't work, but this can be trivially bypassed by using a construct such