#3459 new bug

Opened 22 months ago
Last modified 5 months ago

XSS via malicious .torrent file

Reported by:	jasperla	Owned by:	
Priority:	major	Milestone:	2.1.1
Component:	Web UI	Version:	develop
Keywords:	security xss	Cc:	

Description

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 as `<img src="#" onerror=` or just a hidden, remote iframe which loads the Javascript payload (see the PoC script for an example).

This script creates a PoC torrent to demonstrate the vulnerability: https://gist.github.com/jasperla/4e6e06034e1cc4131f62839b46b697ef the attached screenshot is taken after uploading a .torrent file generated by that script.

Additionally there are several HTML injection bugs, for example in the *Connection Manager*, but these are merely bugs as the local user injects the payload as opposed to a remote attacker who uploads a malicious torrent to a public search engine.

Attachments (1)

Change History (5)

Changed 22 months ago by jasperla

- **Attachment** *deluge xss.png* added

Changed 22 months ago by jasperla — comment:1

- **Keywords** *security xss* added

Changed 10 months ago by Cas — comment:2

Fixed XSS issues in [8ece03677] and [a5503c0c606]

I'll leave open to consider how to implement CSP

Thanks Jasper for reporting and let me know if I missed something or anything else that should be looked at.

Changed 10 months ago by Cas — comment:3

- **Milestone** changed from *needs verified* to *2.1.0*

Changed 5 months ago by Cas — comment:4

- **Milestone** changed from *2.1.0* to *2.1.1*

Ticket retargeted after milestone closed