Marshall-Hallenbeck / **opentrade_0.2.0_domxss_disclosure_1-10-2020**

Last active 3 years ago





OpenTrade Dom-Based XSS Disclosure

opentrade_0.2.0_domxss_disclosure_1-10-2020

```
[Vulnerability Description]
OpenTrade through version 0.2.0 has a Dom-based XSS vulnerability that is executed when an administrator attempts to delete a message that

[Application Description]
OpenTrade is an open source crypto currency exchange that can support over a dozen cryptocurrencies. Its live version can be found at https

[Affected Versions]
The following commit introduced the vulnerability, but OpenTrade did not have a package.json with applicable versioning: https://github.com
Officially version 0.2.0 of OpenTrade is the only "vulnerable" version, as it is the first committed version number in package.json

[Overview]
When an administrator attempts to delete a chat message, a modal is opened asking the administrator to confirm the deletion.
This modal does not HTML or URL encode the message contents, allowing Javascript to be executed in the context of the administrator's brows
Affected line: https://github.com/3s3s/opentrade/blob/4f91391164219da30533453e1ff6800ef2ef3c6b/static_pages/js/index.js#L473
Due to OpenTrade not setting the "token" (session) cookie with the "HTTPOnly" flag, this allows an attacker to steal administrator's sessio

[Proof of Concept]
As a normal user:
*) Submit a chat message with Javascript contents, e.g. <script>alert()</script> (this will not execute in the chat box).
As an administrator:
*) Attempt to delete the message containing Javascript by clicking the X delete button to the right of the message.
*) Clicking this button will trigger the Javascript instantly, as the unencoded message has been loaded into a modal.

[Fix]
Apply encodeURI() to message output
https://github.com/3s3s/opentrade/pull/337

[Other]
CVSS (proposed): 7.6 (High) - https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AC:L/AV:N/A:N/C:H/I:L/PR:L/S:C/UI:R
Vulnerability Type: Dom-Based Cross-Site Scripting (XSS)
Discoverer: Marshall Hallenbeck (@mjhallenbeck)
CVE: CVE-2020-6847 (https://github.com/CVEProject/cvelist/blob/master/2020/6xxx/CVE-2020-6847.json)
```