



CVE-2020-26037

Published on: Not Yet Published

Last Modified on: 11/07/2023 03:20:00 AM UTC

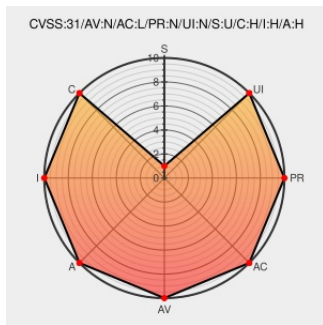
CVE-2020-26037

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Punkbuster](#) from [Evenbalance](#) contain the following vulnerability:

Directory Traversal vulnerability in Server functionality in Even Balance Punkbuster version 1.902 before 1.905 allows remote attackers to execute arbitrary code.

CVE-2020-26037 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|------------------|------------------------|---------------------|---------------------|
| NETWORK | LOW | NONE | NONE |
| Scope | Confidentiality Impact | Integrity Impact | Availability Impact |
| UNCHANGED | HIGH | HIGH | HIGH |

CVE References

| Description | Tags | Link |
|--|---|--|
| Hacking Punkbuster. A Directory Traversal Attack on... by Daniel Prizmant Medium | medium.com text/html | MISC medium.com/@prizmant/hacking-punkbuster-e22e6cf2f36e |
| Responsible on-demand pay Even | even.com text/html | MISC even.com |
| Even Balance, Inc. - PunkBuster Online Countermeasures | punkbuster.com text/html | MISC punkbuster.com |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

