

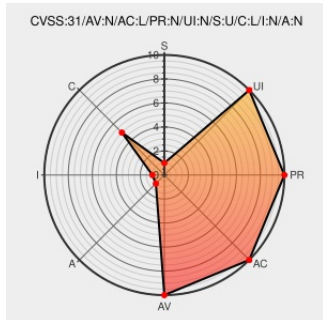


CVE-2022-37146

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2022-37146

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The PlexTrac platform prior to version 1.28.0 allows for username enumeration via HTTP response times on invalid login attempts for users configured to use the PlexTrac authentication provider. Login attempts for valid, unlocked users configured to use PlexTrac as their authentication provider take significantly longer than those for invalid

users, allowing for valid users to be enumerated by an unauthenticated remote attacker. Note that the lockout policy implemented in Plextrac version 1.17.0 makes it impossible to distinguish between valid, locked user accounts and user accounts that do not exist, but does not prevent valid, unlocked users from being enumerated.

CVE-2022-37146 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Pentest Reporting and Collaboration Platform - PlexTrac	plextrac.com text/html	MISC plextrac.com
A PlexTrac Story	www.controlgap.com text/html	MISC www.controlgap.com/blog/a-plextrac-story

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Plextrac	Plextrac	All	All	All	All
cpe:2.3:a:plextrac:plextrac:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-37146 : The PlexTrac platform prior to version 1.28.0 allows for username enumeration via HTTP response ti... twitter.com/i/web/status/1...	2022-09-08 01:03:19
 /r/netcve	CVE-2022-37146	2022-09-08 01:38:54

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report