



CVE-2022-30770

Published on: Not Yet Published

Last Modified on: 10/27/2022 08:23:00 PM UTC

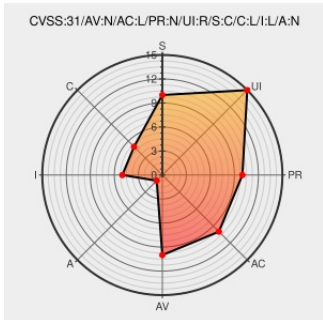
CVE-2022-30770

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Terminalfour versions 8.3.7, 8.3.x versions prior to version 8.3.8 and r 8.2.x versions prior to version 8.2.18.5 or 8.2.18.2.1 are vulnerable to (XSS) vulnerability that could be exploited by an attacker to mislead an administrator and steal their credentials.

CVE-2022-30770 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
	bulletproofsi.com application/pdf	MISC bulletproofsi.com/wp-content/uploads/2022/10/Bulletproof_Vuls_Id_CVE-2022-30770.pdf
Terminalfour 8.2.18.5 Release Notes -	docs.terminalfour.com	MISC docs.terminalfour.com/release-notes/82/185.html

Terminalfour Knowledge Base	text/html	
Terminalfour 8.2.18.2.1 Release Notes - Terminalfour Knowledge Base	docs.terminalfour.com text/html	MISC docs.terminalfour.com/release-notes/82/1821.html
Terminalfour 8.3.8 Release Notes - Terminalfour Knowledge Base	docs.terminalfour.com text/html	MISC docs.terminalfour.com/release-notes/83/8.html
	bulletproofsi.com application/pdf	MISC bulletproofsi.com/wp-content/uploads/2022/08/Bulletproof_Vuls_Id_2022-30770.pdf

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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Terminalfour	Terminalfour	All	All	All	All
cpe:2.3:a:terminalfour:terminalfour:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-30770 : Terminalfour before 8.3.8 allows #XSS, aka RDSM-31817. 8.2.18.2.1 and 8.2.18.5 are also fixed vers... twitter.com/i/web/status/1...	2022-05-16 03:07:08
@threatmeter	CVE-2022-30770 Terminalfour before 8.3.8 allows XSS, aka RDSM-31817. 8.2.18.2.1 and 8.2.18.5 are also fixed version... twitter.com/i/web/status/1...	2022-05-16 23:21:39
/r/netcve	CVE-2022-30770	2022-05-16 04:38:26

← Previous ID

Next ID →

[site](#). This site includes MITRE data granted under the following [license](#).

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