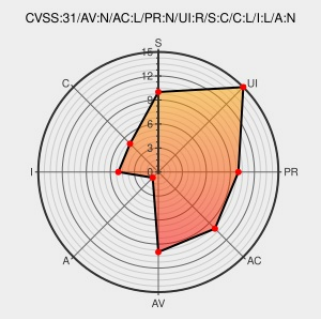
CVE-2022-39197

Published on: Not Yet Published

Last Modified on: 09/22/2022 07:57:00 PM UTC

CVE-2022-39197

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cobalt Strike from Helpsystems contain the following vulnerability:

An XSS (Cross Site Scripting) vulnerability was found in HelpSystems Cobalt Strike through 4.7 that allowed a remote attacker to execute HTML on the Cobalt Strike teamserver. To exploit the vulnerability, one must first inspect a Cobalt Strike payload, and then modify the username field in the payload (or create a new payload with the extracted information and then modify that username field to be malformed).

CVE-2022-39197 has been assigned by 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

CVE References

Description	Tags	Link
Out Of Band Update: Cobalt Strike 4.7.1 | Cobalt Strike	www.cobaltstrike.com text/html	MISC www.cobaltstrike.com/blog/out-of-band-update-cobalt-strike-4-7-1/
Releases Archives - Cobalt Strike Research and Development	www.cobaltstrike.com text/html	MISC www.cobaltstrike.com/blog/tag/release/

There are currently no QIDs associated with this CVE

Exploit/POC from Github

cobaltstrike4.5版本破/解、去除checksum8特征、bypass BeaconEye、修复错误路径泄漏stage、增加totp双因子验证、修复CVE-2022-39197等

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Helpsystems	Cobalt Strike	All	All	All	All

cpe:2.3:a:helpsystems:cobalt_strike:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@caveeroo	Out Of Band Update: Cobalt Strike 4.7.1 cobaltstrike.com/blog/out-of-ba… CVE-2022-39197 would allow an attacker to set a… twitter.com/i/web/status/1…	2022-09-20 15:37:44
@TebbaaX	CVE-2022-39197 cobaltstrike.com/blog/out-of-ba…	2022-09-20 15:50:07
@flanker9527	CVE-2022-39197 Cobalt Strike <= 4.7 RCE The vulnerability can be exploited to achieve RCE without access to the tea… twitter.com/i/web/status/1…	2022-09-21 04:09:35
@jas502n	#CVE-2022-39197 Cobalt Strike <=4.7 RCE cobaltstrike.com/blog/out-of-ba…	2022-09-21 04:12:27
@80vul	cobaltstrike.com/blog/out-of-ba… Cobalt Strike RCE (CVE-2022-39197) and hunting CS by using ZoomEye 80vul.medium.com/identifying-co…	2022-09-21 04:25:40
@cyberkendra	Cobalt Strike XSS to RCE (CVE-2022-39197) bug.cyberkendra.com/2022/09/21/cob… #security #xss #CobaltStrike	2022-09-21 04:34:48
@sirifu4k1	Out Of Band Update: Cobalt Strike 4.7.1 | Cobalt Strike CVE-2022-39197 XSS2RCE ! CS version<=4.7 cobaltstrike.com/blog/out-of-ba…	2022-09-21 04:44:19
@momika233	Out Of Band Update: Cobalt Strike 4.7.1 | Cobalt Strike CVE-2022-39197 XSS2RCE ! CS version<=4.7 cobaltstrike.com/blog/out-of-ba…	2022-09-21 05:44:40
@kladblokje_88	@ali_qushji @briankrebs @jrsofty Cve-2022-39197?	2022-09-21 09:33:39
@buaqbot	「DogCS」简单更新修复fix[CVE-2022-39197]cs_xss ift.tt/A5cOPYI ift.tt/kUtfRJQ	2022-09-21 14:25:21
@TaurusOmar_	Cobalt Strike 4.7.1 | CVE-2022-39197 Vulnerability XSS To RCE | CSversion<=4.7 #cobaltstrike #Infosec #CVE cobaltstrike.com/blog/out-of-ba…	2022-09-21 14:28:24
@buaqbot	CS4.5粗略预防CVE-2022-39197 XSS RCE ift.tt/C07HrUJ ift.tt/KGT1LDH	2022-09-21 14:30:23
@ipssignatures	The vuln CVE-2022-39197 has a tweet created 0 days ago and retweeted 17 times. twitter.com/80vul/status/1… #pow1rtrtwwcve	2022-09-21 20:06:00
@gaetanoz	CVE-2022-39197 cobaltstrike.com/blog/out-of-ba…	2022-09-21 21:52:46

@buffaloverflow	Cobalt Strike CVE-2022-39197. Quite easy to repro from the release notes. Red Teamers, patch your Team Servers ?… twitter.com/i/web/status/1…	2022-09-21 22:30:23
@CyberRaiju	Wonder what the fallout will be with eCrime actors using cracked Cobalt Strike vuln to CVE-2022-39197:… twitter.com/i/web/status/1…	2022-09-21 22:52:38
@sploitus_com	Exploit for CVE-2022-39197 sploitus.com/exploit?id=2A4… #Exploit #Sploitus	2022-09-22 00:27:28
@Herdwolfman	CVE-2022-39197 看上去只要伪造的上线名称中包含xss就可以执行了。 twitter.com/buffaloverflow…	2022-09-22 00:39:20
@CVEreport	CVE-2022-39197 : An #XSS Cross Site Scripting vulnerability was found in HelpSystems Cobalt Strike through 4.7 th… twitter.com/i/web/status/1…	2022-09-22 01:07:24
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-39197 - An XSS (Cross Site Scripting) vulnerability was found in HelpSystems… twitter.com/i/web/status/1…	2022-09-22 01:42:17
@amirdaly0x00	Cobalt Strike 存储型xss漏洞（CVE-2022-39197） dlvr.it/SYmhhD	2022-09-22 04:39:34
@the_yellow_fall	CVE-2022-39197: critical Cobalt Strike bug could lead to RCE attacks securityonline.info/cve-2022-39197… #opensource #infosec #security #pentesting	2022-09-22 04:55:46
@AcooEdi	CVE-2022-39197: critical Cobalt Strike bug could lead to RCE attacks dlvr.it/SYmk78 via securityonline https://t.co/awIpO0nnwr	2022-09-22 05:00:06
@Dinosn	CVE-2022-39197: critical Cobalt Strike bug could lead to RCE attacks securityonline.info/cve-2022-39197…	2022-09-22 05:15:23
@nscrut_	Bad news for all the ransomware gangs and others using cracked copies of Cobalt Strike 4.3 securityonline.info/cve-2022-39197…	2022-09-22 05:17:50
/r/netcve	CVE-2022-39197	2022-09-22 02:38:22

← Previous ID

Next ID→