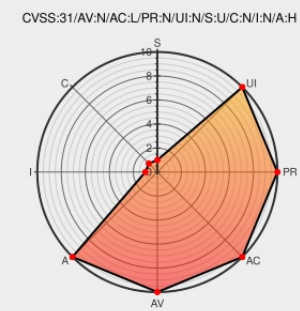
CVE-2021-36798

Published on: 08/09/2021 12:00:00 AM UTC

Last Modified on: 08/17/2021 12:49:00 PM UTC

CVE-2021-36798

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



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

A Denial-of-Service (DoS) vulnerability was discovered in Team Server in HelpSystems Cobalt Strike 4.2 and 4.3. It allows remote attackers to crash the C2 server thread and block beacons' communication with it.

CVE-2021-36798 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Cobalt Strike Release Notes	www.cobaltstrike.com text/html	MISC www.cobaltstrike.com/releasenotes.txt
Hotcobalt - New Cobalt Strike DoS Vulnerability That Lets You Halt Operations - SentinelLabs	labs.sentinelone.com text/html	MISC labs.sentinelone.com/hotcobalt-new-cobalt-strike-dos-vulnerability-that-lets-you-halt-operations/

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

Tool which leverages CVE-2021-36798 (HotCobalt) and related work from SentinelOne to DoS CobaltStrike 4.2 and 4.3 ser…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Helpsystems	Cobalt Strike	4.2	All	All	All
Application	Helpsystems	Cobalt Strike	4.3	All	All	All

cpe:2.3:a:helpsystems:cobalt_strike:4.2:*:*:*:*:*:*:*

cpe:2.3:a:helpsystems:cobalt_strike:4.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@BleepinComputer	@serghei SentinelLabs found the DoS vulnerabilities tracked as CVE-2021-36798 and dubbed Hotcobalt in the latest ve… twitter.com/i/web/status/1…	2021-08-04 13:11:27
@cybersecureny	BleepinComputer: @serghei SentinelLabs found the DoS vulnerabilities tracked as CVE-2021-36798 and dubbed Hotcobalt… twitter.com/i/web/status/1…	2021-08-04 13:15:08
@empressbat	#cybersecurity - Cobalt Strike DoS Vulnerability CVE-2021-36798 discovered by Sentinal Labs There report is here:… twitter.com/i/web/status/1…	2021-08-05 01:08:53
@_ACECODE	Hotcobalt – New Cobalt Strike DoS Vulnerability That Lets You Halt Operations CVE-2021-36798… twitter.com/i/web/status/1…	2021-08-05 10:16:52
@elhackernet	Vulnerabilidad en herramienta Cobalt Strike puede dejar a servidores de botnets y C&C sin servicio (CVE-2021-36798) labs.sentinelone.com/hotcobalt-new-…	2021-08-05 12:10:50
@wearyandroid	One for my APT followers, don't forget to upgrade! Patch that nasty CVE-2021-36798 DDoS and upset criminals 'hacki… twitter.com/i/web/status/1…	2021-08-05 16:17:55
@twelvesec	A Cobalt Strike #DoS #vulnerability (CVE-2021-36798) allows blocking C2 communication. #CyberSecurity, #infosec… twitter.com/i/web/status/1…	2021-08-07 20:34:04
@cyb3rops	#HotCobalt CVE-2021-36798 https://t.co/X4I6oWMA1G	2021-08-07 21:59:17
@ipssignatures	The vuln CVE-2021-36798 has a tweet created 0 days ago and retweeted 10 times. twitter.com/cyb3rops/statu… #pow1rtrtwwcve	2021-08-08 05:06:00
@CVEreport	CVE-2021-36798 : A Denial-of-Service #DoS vulnerability was discovered in Team Server in	2021-08-09

@CVEreport	CVE-2021-36798 : A Denial-of-Service #DoS vulnerability was discovered in Team Server in HelpSystems Cobalt Strik… twitter.com/i/web/status/1…	2021-08-09 13:08:59
/r/hacking	CVE-2021-36798 Cobalt Strike < 4.3 dos	2021-08-19 16:38:25

← Previous ID

Next ID→