Fortra Cobalt Strike User Interface Remote Code Execution Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-42948
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-24 14:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	Cobalt Strike 4.7.1 fails to properly escape HTML tags when they are displayed on Swing components. By injecting crafted

Risk And Classification

EPSS: 0.220640000 probability, percentile 0.958030000 (date 2026-04-29)

CISA KEV: Listed on 2023-03-30; due 2023-04-20; ransomware use Unknown

Problem Types: CWE-116

CISA Known Exploited Vulnerability

Vendor	Fortra
Product	Cobalt Strike
Name	Fortra Cobalt Strike User Interface Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://www.cobaltstrike.com/blog/out-of-band-update-cobalt-strike-4-7-2/; https://nvd.nist.gov/vuln/detail/CVE-2022-42948

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Helpsystems	Cobalt Strike	4.7.1	All	All	All

References

Reference	Source	Link	Ta
How To Fix CVE-2022-42948- A Critical RCE Vulnerability in Cobalt Strike - The Sec Master	MISC	thesecmaster.com	
Cobalt Strike Blog | Cobalt Strike Research and Development	MISC	www.cobaltstrike.com	

HelpSystems Cobalt Strike code execution | CVE-2022-42948 - RedPacket Security	MISC	www.redpacketsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	ke

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

731360 For Vulnerability CVE-2022-42948