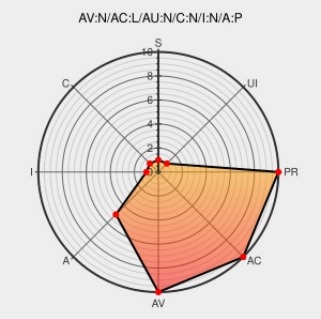
CVE-2005-0478

Published on: 02/19/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:26 PM UTC

CVE-2005-0478

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



Certain versions of Trackercam from Trackercam contain the following vulnerability:

Multiple buffer overflows in TrackerCam 5.12 and earlier allow remote attackers to cause a denial of service and possibly execute arbitrary code via (1) an HTTP request with a long User-Agent header or (2) a long argument to an arbitrary PHP script.

CVE-2005-0478 has been assigned by cve@mitre.org to track the vulnerability

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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF trackercam-useragent-bo(19409)
SecurityFocus	Exploit Vendor Advisory www.securityfocus.com text/html	BUGTRAQ 20050218 Multiple vulnerabilities in TrackerCam 5.12
TrackerCam Multiple Remote Vulnerabilities	Exploit Vendor Advisory cve.report (archive) text/html	BID 12592
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF trackercam-php-bo(19411)

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	Trackercam	Trackercam	All	All	All	All

cpe:2.3:a:trackercam:trackercam:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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