



CVE-2019-14457

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-14457
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-10 18:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	VIVOTEK IP Camera devices with firmware before 0x20x have a stack-based buffer overflow via a crafted HTTP header.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Vivotek	Camera	-	All	All	All
Hardware	Vivotek	Camera	-	All	All	All

References

Reference	Source	Link	Tags
download.vivotek.com/downloadfile/support/cyber-security/vvtk-sa-2019-002-v1.pdf	CONFIRM	download.vivotek.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)