



CVE-2023-33469

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

Summary

CVE	CVE-2023-33469
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-09 20:15:00 UTC
Updated	2023-08-17 01:40:00 UTC
Description	In instances where the screen is visible and remote mouse connection is enabled, KramerAV VIA Connect (2) and VIA Go (2) are vulnerable to a Denial of Service (DoS) attack. An attacker can exploit this vulnerability by sending a specially crafted packet to the device, which will cause the device to crash and become unresponsive. This vulnerability affects all versions of the device that are running the affected firmware. The vulnerability is caused by a buffer overflow in the device's firmware, which allows an attacker to overwrite memory and cause the device to crash. The vulnerability is located in the device's firmware, which is the software that runs on the device's hardware. The vulnerability is caused by a buffer overflow in the device's firmware, which allows an attacker to overwrite memory and cause the device to crash. The vulnerability is located in the device's firmware, which is the software that runs on the device's hardware.

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Kramerav	Via Connect2	-	All	All	All
Operating System	Kramerav	Via Connect2 Firmware	All	All	All	All
Hardware	Kramerav	Via Go2	-	All	All	All
Operating System	Kramerav	Via Go2 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
github.com/Sharpe-nl/CVEs/tree/main/CVE-2023-33469	MISC	github.com	
Kramer Audio Visual Solutions - Kramer	MISC	kramerav.com	
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.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#).

Free CVE JSON API cve.report/api

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