



# CVE-2023-39068

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-39068
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-11 19:15:00 UTC
<b>Updated</b>	2023-09-14 17:45:00 UTC
<b>Description</b>	Buffer Overflow vulnerability in NBD80S09S-KLC v.YK_HZXM_NBD80S09S-KLC_V4.03.R11.7601.Nat.Onvifc.20230414.k

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Hardware	Xiongmaitech	Nb080s09s-klc	-	All
Operating System	Xiongmaitech	Nb080s09s-klc Firmware	yk_hzxm_nbd80s09s-klc_v4.03.r11.7601.nat.onvifc.20230414	All
Hardware	Xiongmaitech	Nbd80n32ra-kl-v3	-	All
Operating System	Xiongmaitech	Nbd80n32ra-kl-v3 Firmware	yk_hzxm_nbd80n32ra-kl_v4.03.r11.7601.nat.onvifc.20220120	All

## References

Reference	Source	Link
Hangzhou Xiongmai Technology Co.,LTD.-Buffer overflow vulnerability exists in Web service firmware of some devices	MISC	<a href="#">www.x</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)