



Tomofun Furbo 360/Furbo Mini GATT Interface URL TF_FQDN.json server-side request forgery

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2025-11648
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-12 22:15:33 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability has been found in Tomofun Furbo 360 and Furbo Mini. Impacted is an unknown function of the file TF_FQDN

Risk And Classification					
Primary CVSS: v4.0 2.9 LOW from cna@vulldb.com					
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X					
Problem Types: CWE-918 CWE-918 Server-Side Request Forgery					
Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	2.9	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H
3.1	cna@vulldb.com	Secondary	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	5.6	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vulldb.com	Secondary	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown	
Attack Vector	Network
Attack Complexity	High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

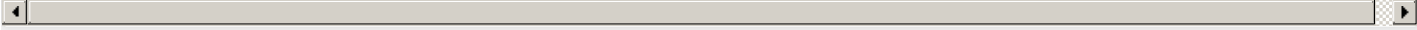
Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H



CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R



NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Furbo	Furbo 360 Dog Camera	All	All	All	All
Operating System	Furbo	Furbo 360 Dog Camera Firmware	All	All	All	All
Hardware	Furbo	Furbo Mini	-	All	All	All
Operating System	Furbo	Furbo Mini Firmware	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Tomofun	Furbo 360	affected n/a	Not specified
CNA	Tomofun	Furbo Mini	affected n/a	Not specified

References			
Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	vuldb.com	Third
vuldb.com	cna@vuldb.com	vuldb.com	Third
vuldb.com	cna@vuldb.com	vuldb.com	Perm
github.com/dead1nfluence/Furbo-Advisories/blob/main/SSRF-via-BLE.md	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Explo
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon



Vendor Comments And Credit

Discovery Credit

CNA: Calvin Star (Software Secured) (en)

CNA: Julian B (Software Secured) (en)

CNA: jTag Labs (VulDB User) (en)

CNA: jTag Labs (VulDB User) (en)

Additional Advisory Data		
Source	Time	Event
CNA	2025-05-15T20:00:00.000Z	Vulnerability found
CNA	2025-06-21T23:00:00.000Z	Vendor informed
CNA	2025-07-03T04:30:00.000Z	Vendor acknowledged
CNA	2025-10-11T00:00:00.000Z	Advisory disclosed
CNA	2025-10-11T02:00:00.000Z	VulDB entry created
CNA	2025-10-20T06:38:16.000Z	VulDB entry last update

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

© [CVE.report](#) 2026 |

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](#)