Telesquare SKT LTE Router SDT-CS3B1 Insecure Direct Object Reference

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-20223
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-16 14:17:52 UTC
Updated	2026-04-14 16:57:27 UTC
Description	Telesquare SKT LTE Router SDT-CS3B1 firmware version 1.2.0 contains an insecure direct object reference vulnerability t

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@vulncheck.com

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

EPSS: 0.000740000 probability, percentile 0.225150000 (date 2026-04-15)

Problem Types: CWE-639 | CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
3.1	disclosure@vulncheck.com	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/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

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Telesquare	Sdt-cs3b1	-	All	All	All
Operating System	Telesquare	Sdt-cs3b1 Firmware	1.2.0	All	All	All

Vendor Declared Affected Products

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Telesquare	SDT-CS3B1	affected 1.2.0	Not specified

References

Reference	Source	Link
packetstormsecurity.com/files/145551	disclosure@vulncheck.com	packetstormsecurity.com
www.exploit-db.com/exploits/43402	disclosure@vulncheck.com	www.exploit-db.com
cxsecurity.com/issue/WLB-2017120297	disclosure@vulncheck.com	cxsecurity.com
www.zeroscience.mk/en/vulnerabilities/ZSL-2017-5445.php	disclosure@vulncheck.com	www.zeroscience.mk
exchange.xforce.ibmcloud.com/vulnerabilities/136993	disclosure@vulncheck.com	exchange.xforce.ibmcloud
www.vulncheck.com/advisories/telesquare-skt-lte-router-sdt-cs3b1-insecure-direc...	disclosure@vulncheck.com	www.vulncheck.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: LiquidWorm as Gjoko Krstic of Zero Science Lab (en)

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 registred 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**