



# USB-based arbitrary memory write vulnerability in ZTE ZX297520V3 soc BootROM

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

## Summary

<b>CVE</b>	CVE-2026-40003
<b>State</b>	PUBLISHED
<b>Assigner</b>	zte
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 02:16:03 UTC
<b>Updated</b>	2026-05-07 02:16:03 UTC
<b>Description</b>	ZTE ZX297520V3 BootROM contains a vulnerability that allows arbitrary memory writes via USB. Attackers can exploit the

## Risk And Classification

**Primary CVSS:** v3.1 5.1 MEDIUM from psirt@zte.com.cn

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

**Problem Types:** CWE-787 | CWE-787 CWE-787 Out-of-bounds write

Version	Source	Type	Score	Severity	Vector
3.1	psirt@zte.com.cn	Secondary	5.1	MEDIUM	CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:L
3.1	CNA	CVSS	5.1	MEDIUM	CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

Low

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ZTE	ZX297520V3 BootROM	affected 7520V3 chip	Not specified

#### References

Reference	Source	Link	Tags
support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/2144487415169560645	psirt@zte.com.cn	<a href="https://support.zte.com.cn">support.zte.com.cn</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analy

#### Vendor Comments And Credit

Discovery Credit

**CNA:** rva3 (en)

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

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)