



CVE-2012-2949

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

Summary

CVE	CVE-2012-2949
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-29 19:55:00 UTC
Updated	2023-11-07 02:11:00 UTC
Description	The ZTE sync_agent program for Android 2.3.4 on the Score M device uses a hardcoded ztex1609523 password to control

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	2.3.4	All	All	All
Operating System	Google	Android	2.3.4	All	All	All
Hardware	Zte	Score M	-	All	All	All
Hardware	Zte	Score M	-	All	All	All

References

Reference	Source	Link	Tags
ZTE confirms security hole in U.S. phone Reuters	MISC	www.reuters.com	
Why Does ZTE's Score M Have a Built-In Backdoor Hole? News & Opinion PCMag.com	MISC	www.pcmag.com	
Why Does ZTE's Score M Have a Built-In Backdoor Hole? News & Opinion PCMag.com		www.pcmag.com	
The Official Lookout Blog ZTE Security Vulnerability	MISC	blog.mylookout.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)