



CVE-2014-0737

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

Summary

CVE	CVE-2014-0737
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-22 21:55:00 UTC
Updated	2014-03-06 04:50:00 UTC
Description	The Cisco Unified IP Phone 7960G 9.2(1) and earlier allows remote attackers to bypass authentication and change trust rel

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Unified Ip Phone 7960g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7960g	All	All	All	All

References

Reference	Source	Link	Tags
tools.cisco.com/security/center/viewAlert.x	CONFIRM	tools.cisco.com	
20140220 Cisco Third-Generation IP Phone CTL Trust Chain Enforcement Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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