



# CVE-2011-1602

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

## Summary

<b>CVE</b>	CVE-2011-1602
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-06-02 20:55:00 UTC
<b>Updated</b>	2011-11-22 03:56:00 UTC
<b>Description</b>	The su utility on Cisco Unified IP Phones 7900 devices (aka TNP phones) with software before 9.0.3 allows local users to g

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Skippy Client Control Protocol Software	1.0(1)	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0(2)	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0(2)	sr1	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0(3)	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0(4)	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0(5)	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0(9)	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0\1\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0\2\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0\2\	sr1	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0\3\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0\4\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0\5\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.0\9\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.1(1)	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.1\1\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	1.2(1)	All	All	All





















Operating System	Cisco	Skippy Client Control Protocol Software	8.3\3\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.3\3\	sr1	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.3\3\	sr2	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.3\5\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.4\1\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.4\1\	sr2	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.4\2\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.4\3\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.4\4\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.5\2\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.5\2\	sr1	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.5\3\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.5\3\	sr1	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.5\4\	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	8.70	All	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	9.0\2\	sr1	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	All	sr2	All	All
Operating System	Cisco	Skippy Client Control Protocol Software	All	sr2	All	All
Hardware	Cisco	Unified Ip Phone 7906	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7906	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7911g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7911g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7931g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7931g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7941g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7941g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7941g-ge	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7941g-ge	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7942g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7942g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7945g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7945g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7961g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7961g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7961g-ge	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7961g-ge	All	All	All	All

Hardware	Cisco	Unified Ip Phone 7962g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7962g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7965g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7965g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7970g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7970g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7971g-ge	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7971g-ge	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7975g	All	All	All	All
Hardware	Cisco	Unified Ip Phone 7975g	All	All	All	All

## References

Reference	Source
72717	OSVDB
Cisco Security Advisory: Multiple Vulnerabilities in Cisco Unified IP Phones 7900 Series [Products & Services] - Cisco Systems	CISCO
Cisco Unified IP Phones 7900 Series (CVE-2011-1602) Privilege Escalation Vulnerability	BID
Cisco Unified IP Phones 7900 Series Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	SECTRACKER
Cisco Unified IP Phone Privilege Escalation and Security Bypass - Secunia.com	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)**