



CVE-2007-1063

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2007-1063
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-22 01:28:00 UTC
Updated	2019-05-23 16:15:00 UTC
Description	The SSH server in Cisco Unified IP Phone 7906G, 7911G, 7941G, 7961G, 7970G, and 7971G, with firmware 8.0(4)SR1 an

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Unified Ip Phone 7906g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7906g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7911g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7911g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7941g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7941g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7961g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7961g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7970g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7970g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7971g	-	All	All	All
Hardware	Cisco	Unified Ip Phone 7971g	-	All	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7906g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7906g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7906g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7911g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7911g	8.0(4)	sr1	All	All

Operating System	Cisco	Unified Ip Phone Firmware 7911g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7941g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7941g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7941g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7961g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7961g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7961g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7970g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7970g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7970g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7971g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7971g	8.0(4)	sr1	All	All
Operating System	Cisco	Unified Ip Phone Firmware 7971g	8.0(4)	sr1	All	All

References

Reference	Source
Cisco Unified IP Conference Station and Unified IP Phone Vulnerabilities	BID
SecurityTracker.com Archives - Cisco IP Phones Default Account Grants Remote Access and Subsequent Privilege Escalation	SECTRACK
Cisco Unified IP Conference Station / IP Phone Default Accounts - Advisories - Secunia	SECUNIA
45246	OSVDB
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO
IBM X-Force Exchange	XF
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](#)