



CVE-2023-20018

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

Summary

CVE	CVE-2023-20018
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-20 07:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an un

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Ip Phones 8832	-	All	All	All
Operating System	Cisco	Ip Phones 8832 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 7800	-	All	All	All
Operating System	Cisco	Ip Phone 7800 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 7811	-	All	All	All
Operating System	Cisco	Ip Phone 7811 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 7821	-	All	All	All
Operating System	Cisco	Ip Phone 7821 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 7832	-	All	All	All
Operating System	Cisco	Ip Phone 7832 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 7841	-	All	All	All
Operating System	Cisco	Ip Phone 7841 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 7861	-	All	All	All
Operating System	Cisco	Ip Phone 7861 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8800	-	All	All	All
Operating System	Cisco	Ip Phone 8800 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8811	-	All	All	All

Operating System	Cisco	Ip Phone 8811 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8821	-	All	All	All
Hardware	Cisco	Ip Phone 8821-ex	-	All	All	All
Operating System	Cisco	Ip Phone 8821-ex Firmware	All	All	All	All
Operating System	Cisco	Ip Phone 8821 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8831	-	All	All	All
Operating System	Cisco	Ip Phone 8831 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8832	-	All	All	All
Operating System	Cisco	Ip Phone 8832 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8841	-	All	All	All
Operating System	Cisco	Ip Phone 8841 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8845	-	All	All	All
Operating System	Cisco	Ip Phone 8845 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8851	-	All	All	All
Operating System	Cisco	Ip Phone 8851 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8861	-	All	All	All
Operating System	Cisco	Ip Phone 8861 Firmware	All	All	All	All
Hardware	Cisco	Ip Phone 8865	-	All	All	All
Operating System	Cisco	Ip Phone 8865 Firmware	All	All	All	All
Hardware	Cisco	Unified Ip Phone 8851nr	-	All	All	All
Operating System	Cisco	Unified Ip Phone 8851nr Firmware	All	All	All	All
Hardware	Cisco	Unified Ip Phone 8865nr	-	All	All	All
Operating System	Cisco	Unified Ip Phone 8865nr Firmware	All	All	All	All
Hardware	Cisco	Wireless Ip Phone 8821	-	All	All	All
Hardware	Cisco	Wireless Ip Phone 8821-ex	-	All	All	All
Operating System	Cisco	Wireless Ip Phone 8821-ex Firmware	All	All	All	All
Operating System	Cisco	Wireless Ip Phone 8821 Firmware	All	All	All	All

References

Reference	Source	Link
Cisco IP Phone 7800 and 8800 Series Web Management Interface Authentication Bypass Vulnerability	MISC	sec.cloudapps.cisco.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730690](#) Cisco IP Phone 7800 and 8800 Series Web Management Interface Authentication Bypass Vulnerability (cisco-sa-ip-phone-auth-bypass-pSqxZRPR)

© [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](#)