



CVE-2006-0179

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2006-0179
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-11 21:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The Cisco IP Phone 7940 allows remote attackers to cause a denial of service (reboot) via a large amount of TCP SYN pac

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Ip Phone 7940	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
Cisco IP Phone 7940 (Reboot) Denial of Service Exploit			af854a3a-2127-422b-91ae-364da2661108	
Cisco - Networking, Cloud, and Cybersecurity Solutions			af854a3a-2127-422b-91ae-364da2661108	
SecurityTracker.com Archives - Cisco 7940/7960 IP Phones Can Be Crashed by Remote Users			af854a3a-2127-422b-91ae-364da2661108	
Cisco IP Phone 7940 Remote Denial of Service Vulnerability			af854a3a-2127-422b-91ae-364da2661108	
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108	
Secunia - Advisories - Cisco IP Phones SYN Flood Device Reload Vulnerability			af854a3a-2127-422b-91ae-364da2661108	
downloads.securityfocus.com/vulnerabilities/exploits/cisco_ip7940_dos.pl			af854a3a-2127-422b-91ae-364da2661108	
www.osvdb.org/22469			af854a3a-2127-422b-91ae-364da2661108	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			af854a3a-2127-422b-91ae-364da2661108	
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.				