CVE-2007-4753

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

Summary

CVE	CVE-2007-4753
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-08 00:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Thomson ST 2030 SIP phone with software 1.52.1 allows remote attackers to cause a denial of service (device hang) v

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: NVD-CWE-Other | 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	Thomson	St 2030 Sip Phone	1.52.1	firmware	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Thomson SpeedTouch 2030 Denial of Service Vulnerabilities - Advisories - Secunia	af854a3a-212
DOS vulnerability on Thomson SIP phone ST 2030 using an empty packet - CXSecurity.com	af854a3a-212
SecurityTracker.com Archives - Thomson ST 2030 SIP Phone Can Be Crashed By Remote Users Sending an Empty Packet	af854a3a-212
[Full-Disclosure] Mailing List Charter	af854a3a-212
IBM X-Force Exchange	af854a3a-212
SecurityTracker.com Archives - Thomson ST 2030 SIP Phone TO URI Processing Bug Lets Remote Users Deny Service	af854a3a-212
[Full-Disclosure] Mailing List Charter	af854a3a-212
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.