# CVE Detail – CVE-2009-1048

The web interface on the snom VoIP phones snom 300, snom 320, snom 360, snom 370, and snom 820 with firmware 6.5 before 6.5.20, 7.1 before 7.1.39, and 7.3 before 7.3.14 allows remote attackers to bypass authentication, and reconfigure the phone or make arbitrary use of the phone, via a (1) http or (2) https request with 127.0.0.1 in the Host header.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.75022

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-290: Authentication Bypass by Spoofing

## CAPEC(s)

* CAPEC-21: Exploitation of Trusted Identifiers
* CAPEC-22: Exploiting Trust in Client
* CAPEC-459: Creating a Rogue Certification Authority Certificate
* CAPEC-461: Web Services API Signature Forgery Leveraging Hash Function Extension Weakness
* CAPEC-473: Signature Spoof
* CAPEC-476: Signature Spoofing by Misrepresentation
* CAPEC-59: Session Credential Falsification through Prediction
* CAPEC-60: Reusing Session IDs (aka Session Replay)
* CAPEC-667: Bluetooth Impersonation AttackS (BIAS)
* CAPEC-94: Adversary in the Middle (AiTM)

## ATT&CK Techniques

* T1557: Adversary-in-the-Middle
* T1539: Steal Web Session Cookie
* T1553.002: Code Signing
* T1134.001: Token Impersonation/Theft
* T1528: Steal Application Access Token
* T1036.001: Invalid Code Signature
* T1550.004: Web Session Cookie
* T1134: Access Token Manipulation

## Used By (Actors/Tools)

* TrickBot (malware)
* BLINDINGCAN (malware)
* Stuxnet (malware)
* WindTail (malware)
* StrongPity (malware)
* Janicab (malware)
* Ecipekac (malware)
* AppleSeed (malware)
* NETWIRE (malware)
* SslMM (malware)
* GreyEnergy (malware)
* Aria-body (malware)
* Emotet (malware)
* BADHATCH (malware)
* Mafalda (malware)
* Okrum (malware)
* TRANSLATEXT (malware)
* Regin (malware)
* Siloscape (malware)
* BlackCat (malware)
* CHIMNEYSWEEP (malware)
* BOOSTWRITE (malware)
* SpicyOmelette (malware)
* LockerGoga (malware)
* Anchor (malware)
* Line Runner (malware)
* Lumma Stealer (malware)
* Duqu (malware)
* Epic (malware)
* Cuba (malware)
* DarkGate (malware)
* Hydraq (malware)
* Gazer (malware)
* Chaes (malware)
* EVILNUM (malware)
* Sagerunex (malware)
* Metamorfo (malware)
* Spica (malware)
* Bandook (malware)
* PipeMon (malware)
* Shamoon (malware)
* BLUELIGHT (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* MegaCortex (malware)
* RTM (malware)
* StrelaStealer (malware)
* Grandoreiro (malware)
* Tarrask (malware)
* GoBear (malware)
* Bazar (malware)
* XLoader (malware)
* Ryuk (malware)
* HermeticWiper (malware)
* MgBot (malware)
* FinFisher (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* REvil (malware)
* TajMahal (malware)
* Raccoon Stealer (malware)
* Daserf (malware)
* MacMa (malware)
* ROADSWEEP (malware)
* SUNSPOT (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* BackConfig (malware)
* Nerex (malware)
* Clop (malware)
* Troll Stealer (malware)
* Ebury (malware)
* ChChes (malware)
* XCSSET (malware)
* KillDisk (malware)
* AppleJeus (malware)
* BADNEWS (malware)
* QakBot (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* Helminth (malware)
* Dok (malware)
* BitPaymer (malware)
* HermeticWizard (malware)
* NPPSPY (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* AADInternals (tool)
* Empire (tool)
* PcShare (tool)
* PoshC2 (tool)
* CSPY Downloader (tool)
* Peirates (tool)
* Pupy (tool)
* QuasarRAT (tool)
* LuminousMoth (intrusion-set)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* APT41 DUST (campaign)
* ArcaneDoor (campaign)
* OilRig (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* APT42 (intrusion-set)
* Sandworm Team (intrusion-set)
* Suckfly (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* Patchwork (intrusion-set)
* APT28 (intrusion-set)
* Darkhotel (intrusion-set)
* APT29 (intrusion-set)
* Operation Honeybee (campaign)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* menuPass (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* FIN8 (intrusion-set)
* Saint Bear (intrusion-set)
* Scattered Spider (intrusion-set)
* Blue Mockingbird (intrusion-set)
* Windshift (intrusion-set)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* HomeLand Justice (campaign)
* C0017 (campaign)
* Lotus Blossom (intrusion-set)
* Evilnum (intrusion-set)
* CopyKittens (intrusion-set)
* Star Blizzard (intrusion-set)
* PROMETHIUM (intrusion-set)

## Affected Products

* cpe:2.3:o:snom:snom\_300\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_300\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_300\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_320\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_320\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_320\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_360\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_360\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_360\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_370\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_370\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_370\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_820\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_820\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:snom:snom\_820\_firmware:\*:\*:\*:\*:\*:\*:\*:\*