# CVE Detail – CVE-2002-0628

The Telnet service for Polycom ViewStation before 7.2.4 does not restrict the number of failed login attempts, which makes it easier for remote attackers to guess usernames and passwords via a brute force attack.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.79704

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-307: Improper Restriction of Excessive Authentication Attempts

## CAPEC(s)

* CAPEC-16: Dictionary-based Password Attack
* CAPEC-49: Password Brute Forcing
* CAPEC-560: Use of Known Domain Credentials
* CAPEC-565: Password Spraying
* CAPEC-600: Credential Stuffing
* CAPEC-652: Use of Known Kerberos Credentials
* CAPEC-653: Use of Known Operating System Credentials

## ATT&CK Techniques

* T1110.001: Password Guessing
* T1558: Steal or Forge Kerberos Tickets
* T1110.003: Password Spraying
* T1078: Valid Accounts
* T1110.004: Credential Stuffing

## Used By (Actors/Tools)

* TrickBot (malware)
* Linux Rabbit (malware)
* Pony (malware)
* Bad Rabbit (malware)
* Emotet (malware)
* P.A.S. Webshell (malware)
* Lucifer (malware)
* China Chopper (malware)
* SeaDuke (malware)
* Duqu (malware)
* Xbash (malware)
* SpeakUp (malware)
* Kinsing (malware)
* Industroyer (malware)
* Dtrack (malware)
* HermeticWizard (malware)
* MailSniper (tool)
* CrackMapExec (tool)
* Indrik Spider (intrusion-set)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Suckfly (intrusion-set)
* Ember Bear (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* APT28 (intrusion-set)
* Cinnamon Tempest (intrusion-set)
* HEXANE (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Leafminer (intrusion-set)
* APT29 (intrusion-set)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* POLONIUM (intrusion-set)
* Leviathan (intrusion-set)
* Akira (intrusion-set)
* LAPSUS$ (intrusion-set)
* Chimera (intrusion-set)
* menuPass (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* APT41 (intrusion-set)
* INC Ransom (intrusion-set)
* GALLIUM (intrusion-set)
* FIN10 (intrusion-set)
* FIN8 (intrusion-set)
* FIN4 (intrusion-set)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* APT28 Nearest Neighbor Campaign (campaign)
* Night Dragon (campaign)
* Agrius (intrusion-set)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* Axiom (intrusion-set)
* Operation MidnightEclipse (campaign)
* C0032 (campaign)
* HomeLand Justice (campaign)
* FIN5 (intrusion-set)
* APT33 (intrusion-set)
* Silent Librarian (intrusion-set)
* APT18 (intrusion-set)
* Carbanak (intrusion-set)
* Star Blizzard (intrusion-set)
* PittyTiger (intrusion-set)

## Affected Products

* cpe:2.3:h:polycom:viewstation\_128:6.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_128:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_512:6.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_512:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_dcp:6.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_dcp:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_fx\_vs4000:4.1.5:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_h.323:6.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_h.323:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_mp:6.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_mp:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_sp\_384:6.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_sp\_384:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_v.35:6.5.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:h:polycom:viewstation\_v.35:7.2:\*:\*:\*:\*:\*:\*:\*