# CVE Detail – CVE-2016-10003

Incorrect HTTP Request header comparison in Squid HTTP Proxy 3.5.0.1 through 3.5.22, and 4.0.1 through 4.0.16 results in Collapsed Forwarding feature mistakenly identifying some private responses as being suitable for delivery to multiple clients.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.75531

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-697: Incorrect Comparison

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-120: Double Encoding
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-15: Command Delimiters
* CAPEC-182: Flash Injection
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-267: Leverage Alternate Encoding
* CAPEC-3: Using Leading 'Ghost' Character Sequences to Bypass Input Filters
* CAPEC-41: Using Meta-characters in E-mail Headers to Inject Malicious Payloads
* CAPEC-43: Exploiting Multiple Input Interpretation Layers
* CAPEC-44: Overflow Binary Resource File
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-52: Embedding NULL Bytes
* CAPEC-53: Postfix, Null Terminate, and Backslash
* CAPEC-6: Argument Injection
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-67: String Format Overflow in syslog()
* CAPEC-7: Blind SQL Injection
* CAPEC-71: Using Unicode Encoding to Bypass Validation Logic
* CAPEC-73: User-Controlled Filename
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-80: Using UTF-8 Encoding to Bypass Validation Logic
* CAPEC-88: OS Command Injection
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities
* CAPEC-92: Forced Integer Overflow

## ATT&CK Techniques

* T1027: Obfuscated Files or Information

## Used By (Actors/Tools)

* TrickBot (malware)
* EKANS (malware)
* SynAck (malware)
* Bumblebee (malware)
* Amadey (malware)
* Orz (malware)
* NOKKI (malware)
* AvosLocker (malware)
* COATHANGER (malware)
* Sardonic (malware)
* Matryoshka (malware)
* Ecipekac (malware)
* AppleSeed (malware)
* BUSHWALK (malware)
* NETWIRE (malware)
* OLDBAIT (malware)
* TEARDROP (malware)
* Turian (malware)
* Action RAT (malware)
* Gootloader (malware)
* PolyglotDuke (malware)
* SombRAT (malware)
* Snip3 (malware)
* RegDuke (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Diavol (malware)
* Siloscape (malware)
* Kazuar (malware)
* CHIMNEYSWEEP (malware)
* FatDuke (malware)
* DRATzarus (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* Conficker (malware)
* Flagpro (malware)
* Green Lambert (malware)
* ISMInjector (malware)
* PUNCHBUGGY (malware)
* POSHSPY (malware)
* MiniDuke (malware)
* Anchor (malware)
* DarkTortilla (malware)
* ROKRAT (malware)
* CORESHELL (malware)
* PlugX (malware)
* Lumma Stealer (malware)
* DustySky (malware)
* Epic (malware)
* Cuba (malware)
* Clambling (malware)
* DarkGate (malware)
* SVCReady (malware)
* Carbanak (malware)
* XTunnel (malware)
* Hydraq (malware)
* Saint Bot (malware)
* Bundlore (malware)
* Trojan.Karagany (malware)
* Shamoon (malware)
* BPFDoor (malware)
* OopsIE (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* SDBbot (malware)
* RTM (malware)
* SodaMaster (malware)
* StrelaStealer (malware)
* Drovorub (malware)
* Kobalos (malware)
* Ryuk (malware)
* Final1stspy (malware)
* FinFisher (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Valak (malware)
* Samurai (malware)
* PoisonIvy (malware)
* NanoCore (malware)
* TajMahal (malware)
* Daserf (malware)
* Carbon (malware)
* Pisloader (malware)
* Ramsay (malware)
* Pillowmint (malware)
* SUNSPOT (malware)
* BoomBox (malware)
* PUNCHTRACK (malware)
* InnaputRAT (malware)
* GrimAgent (malware)
* Lokibot (malware)
* PoetRAT (malware)
* CoinTicker (malware)
* Ebury (malware)
* Maze (malware)
* ComRAT (malware)
* PowerStallion (malware)
* JPIN (malware)
* HTTPBrowser (malware)
* KillDisk (malware)
* AppleJeus (malware)
* SoreFang (malware)
* Industroyer (malware)
* Agent Tesla (malware)
* ECCENTRICBANDWAGON (malware)
* ShadowPad (malware)
* QakBot (malware)
* Hancitor (malware)
* jRAT (malware)
* Dridex (malware)
* Denis (malware)
* Comnie (malware)
* H1N1 (malware)
* SLOWPULSE (malware)
* ADVSTORESHELL (malware)
* Small Sieve (malware)
* ShimRatReporter (tool)
* Sliver (tool)
* CARROTBALL (tool)
* Brute Ratel C4 (tool)
* Remcos (tool)
* Out1 (tool)
* Imminent Monitor (tool)
* MCMD (tool)
* Earth Lusca (intrusion-set)
* Sandworm Team (intrusion-set)
* Ke3chang (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* BackdoorDiplomacy (intrusion-set)
* Kimsuky (intrusion-set)
* Mustang Panda (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Rocke (intrusion-set)
* RedCurl (intrusion-set)
* Windshift (intrusion-set)
* Gamaredon Group (intrusion-set)
* Moonstone Sleet (intrusion-set)
* APT3 (intrusion-set)
* C0017 (campaign)
* APT-C-36 (intrusion-set)
* Gallmaker (intrusion-set)
* BlackOasis (intrusion-set)

## Affected Products

* cpe:2.3:a:squid-cache:squid:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:squid-cache:squid:\*:\*:\*:\*:\*:\*:\*:\*