# CVE Detail – CVE-2009-0152

iChat in Apple Mac OS X 10.5 before 10.5.7 disables SSL for AOL Instant Messenger (AIM) communication in certain circumstances that are inconsistent with the Require SSL setting, which allows remote attackers to obtain sensitive information by sniffing the network.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.69316

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-312: Cleartext Storage of Sensitive Information

## CAPEC(s)

* CAPEC-37: Retrieve Embedded Sensitive Data

## ATT&CK Techniques

* T1005: Data from Local System
* T1552.004: Private Keys

## Used By (Actors/Tools)

* TrickBot (malware)
* BLINDINGCAN (malware)
* RCSession (malware)
* QuietSieve (malware)
* Bumblebee (malware)
* Amadey (malware)
* Proxysvc (malware)
* yty (malware)
* KOPILUWAK (malware)
* Sardonic (malware)
* Misdat (malware)
* Ursnif (malware)
* ThreatNeedle (malware)
* FrameworkPOS (malware)
* GravityRAT (malware)
* Bankshot (malware)
* SharpDisco (malware)
* xCaon (malware)
* Nebulae (malware)
* RainyDay (malware)
* AppleSeed (malware)
* TinyTurla (malware)
* CosmicDuke (malware)
* EnvyScout (malware)
* Crimson (malware)
* Tomiris (malware)
* DUSTTRAP (malware)
* Machete (malware)
* PowerLess (malware)
* Action RAT (malware)
* PingPull (malware)
* WellMess (malware)
* Woody RAT (malware)
* Mafalda (malware)
* AuTo Stealer (malware)
* Hildegard (malware)
* SombRAT (malware)
* FLASHFLOOD (malware)
* FlawedAmmyy (malware)
* LoFiSe (malware)
* MobileOrder (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* Neoichor (malware)
* MarkiRAT (malware)
* Kazuar (malware)
* CHIMNEYSWEEP (malware)
* FatDuke (malware)
* DRATzarus (malware)
* Rising Sun (malware)
* ShimRat (malware)
* Chrommme (malware)
* BADFLICK (malware)
* Flagpro (malware)
* SpicyOmelette (malware)
* Green Lambert (malware)
* China Chopper (malware)
* ROKRAT (malware)
* DarkWatchman (malware)
* BlackMould (malware)
* Bisonal (malware)
* Rover (malware)
* LightNeuron (malware)
* Clambling (malware)
* DarkGate (malware)
* Mongall (malware)
* SVCReady (malware)
* FoggyWeb (malware)
* Hydraq (malware)
* CreepyDrive (malware)
* Caterpillar WebShell (malware)
* USBferry (malware)
* Latrodectus (malware)
* Saint Bot (malware)
* CharmPower (malware)
* Uroburos (malware)
* Bandook (malware)
* KONNI (malware)
* RAPIDPULSE (malware)
* DnsSystem (malware)
* KGH\_SPY (malware)
* Ixeshe (malware)
* BoxCaon (malware)
* NightClub (malware)
* Crutch (malware)
* SDBbot (malware)
* Hikit (malware)
* WellMail (malware)
* RawPOS (malware)
* ZxxZ (malware)
* Drovorub (malware)
* Shark (malware)
* Bazar (malware)
* BadPatch (malware)
* Cryptoistic (malware)
* MgBot (malware)
* ccf32 (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Samurai (malware)
* PinchDuke (malware)
* Milan (malware)
* OSX\_OCEANLOTUS.D (malware)
* Taidoor (malware)
* Cyclops Blink (malware)
* PoisonIvy (malware)
* TajMahal (malware)
* Raccoon Stealer (malware)
* IPsec Helper (malware)
* DanBot (malware)
* Calisto (malware)
* Ramsay (malware)
* Pillowmint (malware)
* MacMa (malware)
* FunnyDream (malware)
* SysUpdate (malware)
* OutSteel (malware)
* PUNCHTRACK (malware)
* GrimAgent (malware)
* StealBit (malware)
* ZxShell (malware)
* SLIGHTPULSE (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Kinsing (malware)
* njRAT (malware)
* IceApple (malware)
* metaMain (malware)
* SideTwist (malware)
* Mis-Type (malware)
* XCSSET (malware)
* Octopus (malware)
* STARWHALE (malware)
* Pcexter (malware)
* Kevin (malware)
* Pasam (malware)
* POWERSTATS (malware)
* BADNEWS (malware)
* Linfo (malware)
* Goopy (malware)
* QakBot (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* jRAT (malware)
* Dtrack (malware)
* Zox (malware)
* StrifeWater (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* NPPSPY (tool)
* PowerSploit (tool)
* AADInternals (tool)
* Empire (tool)
* PcShare (tool)
* Brute Ratel C4 (tool)
* Out1 (tool)
* Forfiles (tool)
* MCMD (tool)
* Mimikatz (tool)
* esentutl (tool)
* Koadic (tool)
* QuasarRAT (tool)
* Wevtutil (tool)
* LuminousMoth (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)
* Aquatic Panda (intrusion-set)
* Inception (intrusion-set)
* Operation CuckooBees (campaign)
* Sandworm Team (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* CostaRicto (campaign)
* TeamTNT (intrusion-set)
* FIN6 (intrusion-set)
* Patchwork (intrusion-set)
* APT28 (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Magic Hound (intrusion-set)
* APT29 (intrusion-set)
* Operation Honeybee (campaign)
* Andariel (intrusion-set)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* Kimsuky (intrusion-set)
* LAPSUS$ (intrusion-set)
* ToddyCat (intrusion-set)
* menuPass (intrusion-set)
* Operation Dream Job (campaign)
* Stealth Falcon (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* CURIUM (intrusion-set)
* Windigo (intrusion-set)
* RedCurl (intrusion-set)
* Frankenstein (campaign)
* Threat Group-3390 (intrusion-set)
* Gamaredon Group (intrusion-set)
* Night Dragon (campaign)
* Agrius (intrusion-set)
* Axiom (intrusion-set)
* Dark Caracal (intrusion-set)
* APT3 (intrusion-set)
* Operation MidnightEclipse (campaign)
* APT1 (intrusion-set)
* C0017 (campaign)
* Cutting Edge (campaign)
* C0026 (campaign)

## Affected Products

* cpe:2.3:o:apple:mac\_os\_x:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:apple:mac\_os\_x\_server:\*:\*:\*:\*:\*:\*:\*:\*