# CVE Detail – CVE-2007-4961

The login\_to\_simulator method in Linden Lab Second Life, as used by the secondlife:// protocol handler and possibly other Second Life login mechanisms, sends an MD5 hash in cleartext in the passwd field, which allows remote attackers to login to an account by sniffing the network and then sending this hash to a Second Life authentication server.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.57703

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-311: Missing Encryption of Sensitive Data

## CAPEC(s)

* CAPEC-157: Sniffing Attacks
* CAPEC-158: Sniffing Network Traffic
* CAPEC-204: Lifting Sensitive Data Embedded in Cache
* CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies
* CAPEC-37: Retrieve Embedded Sensitive Data
* CAPEC-383: Harvesting Information via API Event Monitoring
* CAPEC-384: Application API Message Manipulation via Man-in-the-Middle
* CAPEC-385: Transaction or Event Tampering via Application API Manipulation
* CAPEC-386: Application API Navigation Remapping
* CAPEC-387: Navigation Remapping To Propagate Malicious Content
* CAPEC-388: Application API Button Hijacking
* CAPEC-477: Signature Spoofing by Mixing Signed and Unsigned Content
* CAPEC-609: Cellular Traffic Intercept
* CAPEC-65: Sniff Application Code

## ATT&CK Techniques

* T1539: Steal Web Session Cookie
* T1040: Network Sniffing
* T1005: Data from Local System
* T1552.004: Private Keys
* T1111: Multi-Factor Authentication Interception
* T1056.004: Credential API Hooking

## Used By (Actors/Tools)

* TrickBot (malware)
* cd00r (malware)
* BLINDINGCAN (malware)
* RCSession (malware)
* QuietSieve (malware)
* Bumblebee (malware)
* Amadey (malware)
* JumbledPath (malware)
* RDFSNIFFER (malware)
* Proxysvc (malware)
* NOKKI (malware)
* yty (malware)
* KOPILUWAK (malware)
* VersaMem (malware)
* Sardonic (malware)
* Misdat (malware)
* Ursnif (malware)
* ThreatNeedle (malware)
* Zeus Panda (malware)
* FrameworkPOS (malware)
* GravityRAT (malware)
* Bankshot (malware)
* SharpDisco (malware)
* xCaon (malware)
* Nebulae (malware)
* RainyDay (malware)
* AppleSeed (malware)
* TinyTurla (malware)
* J-magic (malware)
* CosmicDuke (malware)
* EnvyScout (malware)
* Emotet (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)
* TRANSLATEXT (malware)
* Regin (malware)
* Line Dancer (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)
* Lumma Stealer (malware)
* Sykipot (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)
* Chaes (malware)
* CharmPower (malware)
* EVILNUM (malware)
* Uroburos (malware)
* Spica (malware)
* Bandook (malware)
* KONNI (malware)
* RAPIDPULSE (malware)
* DnsSystem (malware)
* BLUELIGHT (malware)
* KGH\_SPY (malware)
* Ixeshe (malware)
* BoxCaon (malware)
* NightClub (malware)
* Crutch (malware)
* SDBbot (malware)
* Hikit (malware)
* Grandoreiro (malware)
* WellMail (malware)
* RawPOS (malware)
* ZxxZ (malware)
* Drovorub (malware)
* Shark (malware)
* Bazar (malware)
* BadPatch (malware)
* MESSAGETAP (malware)
* XLoader (malware)
* Cryptoistic (malware)
* MgBot (malware)
* ccf32 (malware)
* Zebrocy (malware)
* FinFisher (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)
* Carberp (malware)
* Pillowmint (malware)
* MacMa (malware)
* FunnyDream (malware)
* SysUpdate (malware)
* OutSteel (malware)
* PUNCHTRACK (malware)
* GrimAgent (malware)
* StealBit (malware)
* ZxShell (malware)
* SLIGHTPULSE (malware)
* Penquin (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)
* SLOWPULSE (malware)
* Zox (malware)
* StrifeWater (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* NPPSPY (tool)
* PowerSploit (tool)
* Impacket (tool)
* AADInternals (tool)
* Empire (tool)
* PcShare (tool)
* PoshC2 (tool)
* Brute Ratel C4 (tool)
* Out1 (tool)
* Forfiles (tool)
* MCMD (tool)
* Responder (tool)
* Mimikatz (tool)
* NBTscan (tool)
* esentutl (tool)
* Koadic (tool)
* QuasarRAT (tool)
* Wevtutil (tool)
* LuminousMoth (intrusion-set)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Inception (intrusion-set)
* APT42 (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)
* Chimera (intrusion-set)
* ToddyCat (intrusion-set)
* menuPass (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* Operation Dream Job (campaign)
* Stealth Falcon (intrusion-set)
* DarkVishnya (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* PLATINUM (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)
* Leviathan Australian Intrusions (campaign)
* Salt Typhoon (intrusion-set)
* Axiom (intrusion-set)
* Dark Caracal (intrusion-set)
* APT3 (intrusion-set)
* Operation MidnightEclipse (campaign)
* APT1 (intrusion-set)
* C0017 (campaign)
* APT33 (intrusion-set)
* Cutting Edge (campaign)
* Lotus Blossom (intrusion-set)
* Evilnum (intrusion-set)
* Star Blizzard (intrusion-set)
* C0026 (campaign)

## Affected Products

* cpe:2.3:a:lindenlab:second\_life:-:\*:\*:\*:\*:\*:\*:\*