# CVE Detail – CVE-2003-0174

The LDAP name service (nsd) in IRIX 6.5.19 and earlier does not properly verify if the USERPASSWORD attribute has been provided by an LDAP server, which could allow attackers to log in without a password.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.57618

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-346: Origin Validation Error

## CAPEC(s)

* CAPEC-111: JSON Hijacking (aka JavaScript Hijacking)
* CAPEC-141: Cache Poisoning
* CAPEC-142: DNS Cache Poisoning
* CAPEC-160: Exploit Script-Based APIs
* CAPEC-21: Exploitation of Trusted Identifiers
* 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-510: SaaS User Request Forgery
* CAPEC-59: Session Credential Falsification through Prediction
* CAPEC-60: Reusing Session IDs (aka Session Replay)
* CAPEC-75: Manipulating Writeable Configuration Files
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-89: Pharming

## ATT&CK Techniques

* T1539: Steal Web Session Cookie
* T1134.001: Token Impersonation/Theft
* T1528: Steal Application Access Token
* T1584.002: DNS Server
* T1550.004: Web Session Cookie
* T1557.002: ARP Cache Poisoning
* T1134: Access Token Manipulation

## Used By (Actors/Tools)

* Stuxnet (malware)
* AppleSeed (malware)
* SslMM (malware)
* Aria-body (malware)
* Emotet (malware)
* BADHATCH (malware)
* Mafalda (malware)
* Okrum (malware)
* TRANSLATEXT (malware)
* Siloscape (malware)
* BlackCat (malware)
* Lumma Stealer (malware)
* Duqu (malware)
* Cuba (malware)
* DarkGate (malware)
* Hydraq (malware)
* Chaes (malware)
* EVILNUM (malware)
* Sagerunex (malware)
* Spica (malware)
* Shamoon (malware)
* BLUELIGHT (malware)
* MegaCortex (malware)
* Grandoreiro (malware)
* Tarrask (malware)
* XLoader (malware)
* Ryuk (malware)
* HermeticWiper (malware)
* MgBot (malware)
* FinFisher (malware)
* Cobalt Strike (malware)
* REvil (malware)
* TajMahal (malware)
* Raccoon Stealer (malware)
* SUNSPOT (malware)
* XCSSET (malware)
* KillDisk (malware)
* QakBot (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* BitPaymer (malware)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* Peirates (tool)
* Pupy (tool)
* LuminousMoth (intrusion-set)
* SolarWinds Compromise (campaign)
* APT42 (intrusion-set)
* Sandworm Team (intrusion-set)
* FIN6 (intrusion-set)
* APT28 (intrusion-set)
* APT29 (intrusion-set)
* Kimsuky (intrusion-set)
* LAPSUS$ (intrusion-set)
* FIN8 (intrusion-set)
* Scattered Spider (intrusion-set)
* Blue Mockingbird (intrusion-set)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* HomeLand Justice (campaign)
* C0017 (campaign)
* Lotus Blossom (intrusion-set)
* Evilnum (intrusion-set)
* Cleaver (intrusion-set)
* Star Blizzard (intrusion-set)

## Affected Products

* cpe:2.3:o:sgi:irix:\*:\*:\*:\*:\*:\*:\*:\*