# CVE Detail – CVE-2007-4150

The Visionsoft Audit on Demand Service (VSAOD) in Visionsoft Audit 12.4.0.0 uses weak cryptography (XOR) when (1) transmitting passwords, which allows remote attackers to obtain sensitive information by sniffing the network; and (2) storing passwords in the configuration file, which allows local users to obtain sensitive information by reading this file.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.76858

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-327: Use of a Broken or Risky Cryptographic Algorithm

## CAPEC(s)

* CAPEC-20: Encryption Brute Forcing
* CAPEC-459: Creating a Rogue Certification Authority Certificate
* CAPEC-473: Signature Spoof
* CAPEC-475: Signature Spoofing by Improper Validation
* CAPEC-608: Cryptanalysis of Cellular Encryption
* CAPEC-614: Rooting SIM Cards
* CAPEC-97: Cryptanalysis

## ATT&CK Techniques

* T1553.002: Code Signing
* T1036.001: Invalid Code Signature

## Used By (Actors/Tools)

* TrickBot (malware)
* BLINDINGCAN (malware)
* Stuxnet (malware)
* WindTail (malware)
* StrongPity (malware)
* Janicab (malware)
* Ecipekac (malware)
* NETWIRE (malware)
* GreyEnergy (malware)
* Regin (malware)
* CHIMNEYSWEEP (malware)
* BOOSTWRITE (malware)
* SpicyOmelette (malware)
* LockerGoga (malware)
* Anchor (malware)
* Lumma Stealer (malware)
* Epic (malware)
* Gazer (malware)
* Metamorfo (malware)
* Bandook (malware)
* PipeMon (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* RTM (malware)
* StrelaStealer (malware)
* GoBear (malware)
* Bazar (malware)
* HermeticWiper (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Daserf (malware)
* MacMa (malware)
* ROADSWEEP (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* BackConfig (malware)
* Nerex (malware)
* Clop (malware)
* Troll Stealer (malware)
* Ebury (malware)
* ChChes (malware)
* AppleJeus (malware)
* BADNEWS (malware)
* QakBot (malware)
* Gelsemium (malware)
* Helminth (malware)
* HermeticWizard (malware)
* PcShare (tool)
* CSPY Downloader (tool)
* QuasarRAT (tool)
* LuminousMoth (intrusion-set)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* APT41 DUST (campaign)
* OilRig (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* Suckfly (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* Patchwork (intrusion-set)
* Darkhotel (intrusion-set)
* Operation Honeybee (campaign)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* menuPass (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* Saint Bear (intrusion-set)
* Scattered Spider (intrusion-set)
* Windshift (intrusion-set)
* CopyKittens (intrusion-set)
* PROMETHIUM (intrusion-set)

## Affected Products

* cpe:2.3:a:visionsoft:audit:12.4.0.0:\*:\*:\*:\*:\*:\*:\*