# CVE Detail – CVE-2005-4900

SHA-1 is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of SHA-1 in TLS 1.2. NOTE: this CVE exists to provide a common identifier for referencing this SHA-1 issue; the existence of an identifier is not, by itself, a technology recommendation.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.44443

## CVSS Scoring

CVSS v3.0 Score: 5.9

Severity: MEDIUM

## Mapped CWE(s)

* CWE-326: Inadequate Encryption Strength

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-192: Protocol Analysis
* CAPEC-20: Encryption Brute Forcing

## ATT&CK Techniques

* T1110: Brute Force

## Used By (Actors/Tools)

* Chaos (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Kinsing (malware)
* QakBot (malware)
* PoshC2 (tool)
* CrackMapExec (tool)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:a:google:chrome:\*:\*:\*:\*:\*:\*:\*:\*