CVE-2005-4900

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2005-4900
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-14 16:59:00 UTC
Updated	2020-12-09 09:15:00 UTC
Description	SHA-1 is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demo

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

References

Reference
McAfee Security Bulletin - Database Security update fixes one vulnerability (CVE-2020-7339)
Google Online Security Blog: Announcing the first SHA1 collision
At death's door for years, widely used SHA1 function is now dead | Ars Technica
SHA-0/SHA-1 Reduced Operation Digest Collision Weakness
SHAttered
SHA-1 Broken - Schneier on Security
Cryptology ePrint Archive: Report 2007/474
The Shappening
Google Online Security Blog: An update on SHA-1 certificates in Chrome
CWI and Google announce first collision for Industry Security Standard SHA-1 | CWI Amsterdam | Research in mathematics and computer sci
Schneier on Security: New Cryptanalytic Results Against SHA-1
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**