

CVE-2020-14871

Oracle Solaris and Zettabyte File System (ZFS) Unspecified Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

Vulnerability in the Oracle Solaris product of Oracle Systems (component: Pluggable authentication module). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris.

EVRS

82/100

Urgent priority

CVSS V3.1

10.0

Critical · NVD

EPSS

0.802

99.62nd percentile · FIRST

CISA DEADLINE

May 3, 2022

KEV since 2021 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.802 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Note: This CVE is not exploitable for Solaris 11.1 and later releases, and ZFSS 8.7 and later releases, thus the CVSS Base Score is 0.0. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
solaris	≥ 10 < 11.1 9	11.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-7pcp-8fjh-246q
NVD nvd.nist.gov/vuln/detail/CVE-2020-14871**Additional guidance** oracle.com/security-alerts/cpuoct2020.html
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2020-7007**Current data** evulnable.com/vulnerability-management/cve/CVE-2020-14871

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.