CVE-2019-3010

Oracle Solaris Privilege Escalation Vulnerability

CISA KEV since May 25, 2022 | Actively exploited | Public exploit module (Metasploit)

Vulnerability in the Oracle Solaris product of Oracle Systems (component: XScreenSaver). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes 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	CVSS V3.1	EPSS	CISA DEADLINE
75/100 Urgent priority	8.8 High · NVD	0.134 96.4th percentile · FIRST	Jun 15, 2022 KEV since 2022 · 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	0.134 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 8.8	− 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

CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
solaris	11	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-w255-p3v2-q6mg
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2019-3010
NVD nvd.nist.gov/vuln/detail/CVE-2019-3010
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-12649

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