

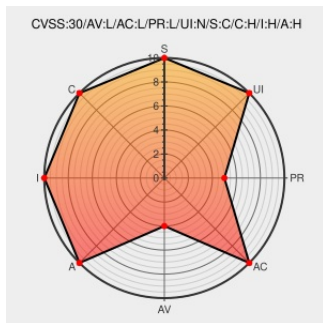


CVE-2020-2696

Published on: 01/15/2020 12:00:00 AM UTC

Last Modified on: 10/25/2022 05:52:00 PM UTC

CVE-2020-2696

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Solaris](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). The supported version that is affected is 10. 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. 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).

CVE-2020-2696 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Oracle Corporation - Solaris Operating System** version = 10

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SunOS 5.10 Generic_147148-26 Local Privilege Escalation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/155963/SunOS-5.10-Generic_147148-26-Local-Privilege-Escalation.html
oss-security - CVE-2020-2656, CVE-2020-2696 - Multiple vulnerabilities in Oracle Solaris	www.openwall.com text/html	 MLIST [oss-security] 20200120 CVE-2020-2656, CVE-2020-2696 - Multiple vulnerabilities in Oracle Solaris
Common Desktop Environment 2.3.1 Buffer Overflow ≈ Packet Storm	Exploit Patch Third Party Advisory packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/155991/Common-Desktop-Environment-2.3.1-Buffer-Overflow.html
Bugtraq: CVE-2020-2696 - Local privilege escalation via CDE dtsession	Exploit Mailing List Third Party Advisory seclists.org text/html	 BUGTRAQ 20200117 CVE-2020-2696 - Local privilege escalation via CDE dtsession
Full Disclosure: CVE-2020-2696 - Local privilege escalation via CDE dtsession	Exploit Third Party Advisory seclists.org text/html	 FULLDISC 20200117 CVE-2020-2696 - Local privilege escalation via CDE dtsession
Oracle Critical Patch Update Advisory - January 2020	Patch Vendor Advisory www.oracle.com text/html	 MISC www.oracle.com/security-alerts/cpujan2020.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[690065](#) Free Berkeley Software Distribution (FreeBSD) Security Update for x11/cde (848bdd06-f93a-11eb-9f7d-206a8a720317)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Oracle	Solaris	10	All	All	All
Operating System	Oracle	Solaris	10	All	All	All
cpe:2.3:o:oracle:solaris:10:*:*:*:*:*						
cpe:2.3:o:oracle:solaris:10:*:*:*:*:*						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID		Next ID→

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)