CVE-2020-2696 - Local privilege escalation via CDE dtsession

From: Marco Ivaldi <marco.ivaldi () mediaservice net>
Date: Wed, 15 Jan 2020 13:57:08 +0000

```
Dear Full Disclosure,

Please find attached an advisory for the following vulnerability, fixed in Oracle's Critical Patch Update (CPU) of
January 2020:

"A buffer overflow in the CheckMonitor() function in the Common Desktop Environment 2.3.1 and earlier and 1.6 and
earlier, as distributed with Oracle Solaris 10 1/13 (Update 11) and earlier, allows local users to gain root
privileges
via a long palette name passed to dtsession in a malicious .Xdefaults file."

For further information, please refer to:
https://techblog.mediaservice.net/2020/01/local-privilege-escalation-via-cde-dtsession/
https://github.com/0xdea/exploits/blob/master/solaris/raptor_dtsession_ipa.c

Regards,

--
Marco Ivaldi, Offensive Security Manager
CISSP, OSCP, QSA, ASV, OPSA, OPST, OWSE, LA27001, PRINCE2F
@Mediaservice.net S.r.l. con Socio Unico
https://www.mediaservice.net/
Tel: +39 011 19016595 | Fax: +39 011 3246497
```

Attachment: `2020-02-cde-dtsession.txt`
Description: 2020-02-cde-dtsession.txt

By Date By Thread

Current thread:

CVE-2020-2696 - Local privilege escalation via CDE dtsession ***Marco Ivaldi (Jan 17)***