Date: Wed, 15 Apr 2020 14:42:34 +0000
From: Marco Ivaldi <marco.ivaldi@...iaservice.net>
To: "Fulldisclosure@...lists.org" <Fulldisclosure@...lists.org>,
"oss-security@...ts.openwall.com" <oss-security@...ts.openwall.com>
Subject: CVE-2020-2771, CVE-2020-2851, CVE-2020-2944 - Multiple
vulnerabilities in Oracle Solaris

Hello,

Please find attached 3 recent advisories for the following vulnerabilities, fixed in Oracle's Critical Patch Update (CPU) of April 2020:

CVE-2020-2771. A difficult to exploit heap-based buffer overflow in setuid root whodo and w binaries distributed with Solaris allows local users to corrupt memory and potentially execute arbitrary code in order to escalate privileges.

CVE-2020-2851. A difficult to exploit stack-based buffer overflow in the _DtCreateDtDirs() function in the Common Desktop Environment version distributed with Oracle Solaris 10 1/13 (Update 11) and earlier may allow local users to corrupt memory and potentially execute arbitrary code in order to escalate privileges via a long X11 display name. The vulnerable function is located in the libDtSvc library and can be reached by executing the setuid program dtsession.

CVE-2020-2944. A buffer overflow in the _SanityCheck() function in the Common Desktop Environment version distributed with Oracle Solaris 10 1/13 (Update 11) and earlier allows local users to gain root privileges via a long calendar name or calendar owner passed to sdtcm_convert in a malicious calendar file.

For further details and some background information, please refer to:
https://techblog.mediaservice.net/2020/04/cve-2020-2944-local-privilege-escalation-via-cde-sdtcm_convert/
https://github.com/0xdea/exploits/blob/master/solaris/raptor_sdtcm_conv.c
https://0xdeadbeef.info/

PS. It looks like Bugtraq is not accepting posts anymore: it finally happened, the end of an era...

--
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/

View attachment "2020-05-cde-sdtcm_convert.txt**" of type "**text/plain**" (3762 bytes)**

View attachment "2020-06-cde-libDtSvc.txt**" of type "**text/plain**" (6462 bytes)**

View attachment "2020-07-solaris-whodo-w.txt**" of type "**text/plain**" (8786 bytes)**