

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

IOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

Common Desktop Environment 2.3.1 Buffer Overflow

Authored by Marco Ivaldi

Posted Jan 17, 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. Note that Oracle Solaris CDE is based on the original CDE 1.x train, which is different from the CDE 2.x codebase that was later open sourced. Most notably, the vulnerable buffer in the Oracle Solaris CDE is stack-based, while in the open source version it is heap-based.

tags | exploit, overflow, local, root systems | solaris advisories | CVE-2020-2696

SHA-256 | d25b46d4823e23cf621654e72fc9113aa59c9c5cd75e5f0f889790d85edd1e5 Download | Favorite | View

Related Files

Share This

Like Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror

Download

@Mediaservice.net Security Advisory #2020-02 (last updated on 2020-01-15)

Title: Local privilege escalation via CDE dtsession
Application: Common Desktop Environment 2.3.1 and earlier
Common Desktop Environment 1.6 and earlier
Platforms: Oracle Solaris 10 1/13 (Update 11) and earlier
Other platforms are potentially affected (see below)
Description: A local attacker can gain root privileges by exploiting a buffer overflow in CDE dtsession
Author: Marco Ivaldi <marco.ivaldi@mediaservice.net>
Vendor Status: Oracle <secalert_us@oracle.com> notified on 2019-11-13
CERT/CC notified on 2019-12-09 (tracking VU#308289)
CVE Name: CVE-2020-2696
CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:IC/C:H/I:H/A:H (Base Score: 8.8)
References: https://github.com/Oxdea/advisories/blob/master/2020-02-cde-dtsession.txt
https://www.oracle.com/security-alerts/cpujan2020.html
https://sourceforge.net/p/cdesktopenv/wiki/Home/
https://www.oracle.com/technetwork/server-storage/solaris10/
https://www.mediaservice.net/
https://0xdeadbeef.info/

1. Abstract

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.

Note that Oracle Solaris CDE is based on the original CDE 1.x train, which is different from the CDE 2.x codebase that was later open sourced. Most notably, the vulnerable buffer in the Oracle Solaris CDE is stack-based, while in the open source version it is heap-based.

2. Example Attack Session.

```
bash-3.2$ cat /etc/release
Oracle Solaris 10 1/13 s10x_u11w02_24a X86
Copyright (c) 1983, 2013, Oracle and/or its Affiliates. All rights reserved.
Assembled 17 January 2013

bash-3.2$ uname -a
SunOS notalgia 5.10 Generic_147148-26 i86pc i386 i86pc
bash-3.2$ id
uid=54322(raptor) gid=1(other)
bash-3.2$ gcc raptor_dtsession_ipa.c -o raptor_dtsession_ipa -Wall
bash-3.2$ ./raptor_dtsession_ipa 192.168.1.1:0
raptor_dtsession_ipa.c - CDE dtsession LPE for Solaris/Intel
Copyright (c) 2019-2020 Marco Ivaldi <raptor@0xdeadbeef.info>

Using 91 PLATFORM : i86pc (5.10)
Using stack base : 0x8047fff
Using rwx_mem address : 0xfeffa004
Using payload address : 0x8047dff
Using strcpy() address : 0xfef26a0

# id
uid=0(root) gid=1(other)
```

3. Affected Platforms.

All platforms shipping the Common Desktop Environment are potentially affected. This includes:

- * Oracle Solaris 10 1/13 (Update 11) and earlier [default installation]

According to the CDE Wiki, the following platforms are officially supported:

- * All Official Ubuntu variants 12.04 - 18.04
- * Debian 6, 7, 8, 9
- * Fedora 17 at least
- * Archlinux
- * Red Hat
- * Slackware 14.0
- * OpenBSD
- * NetBSD
- * FreeBSD 9.2, 10.x, 11.x
- * openSUSE Tumbleweed (gcc7)
- * openSUSE Leap 4.2 (gcc4)
- * SUSE 12 SP3 (gcc4)
- * Solaris, OpenIndiana

4. Fix.

The maintainers of the open source CDE 2.x version have issued the following patches for this vulnerability:
https://sourceforge.net/p/cdesktopenv/mailman/message/36900154/
https://sourceforge.net/p/cdesktopenv/code/ci/6b32246d06ab16fd7897dc344db69d0957f3ae08/

Oracle, which maintains a different CDE codebase based on the 1.x train, has assigned the tracking# 8121688 and has released a fix for all affected and supported versions of Solaris in their Critical Patch Update (CPO) of January 2020.

As a workaround, it is also possible to remove the setuid bit from the vulnerable executable as follows (note that this might prevent it from working properly):

```
bash-3.2$ chmod -s /usr/dt/bin/dtsession
```

Please note that during the audit many other potentially exploitable bugs have surfaced in dtsession and in the Common Desktop Environment in general. Therefore, removing the setuid bit from all CDE binaries is recommended, regardless of patches released by vendors.

5. Proof of Concept.

An exploit for Oracle Solaris 10 1/13 (Update 11) Intel has been developed as a proof of concept. It can be downloaded from:

https://github.com/Oxdea/exploits/blob/master/solaris/raptor_dtsession_ipa.c

Copyright (c) 2020 Marco Ivaldi and @Mediaservice.net. All rights reserved.

[Login](#) or [Register](#) to add favorites

[Spoof](#) (2,166) [SUSE](#) (1,444)
[SQL Injection](#) (16,102) [Ubuntu](#) (8,199)
[TCP](#) (2,379) [UNIX](#) (9,159)
[Trojan](#) (686) [UnixWare](#) (185)
[UDP](#) (876) [Windows](#) (6,511)
[Virus](#) (662) [Other](#)
[Vulnerability](#) (31,136)
[Web](#) (9,365)
[Whitepaper](#) (3,729)
[x86](#) (946)
[XSS](#) (17,494)
[Other](#)



© 2022 Packet Storm. All rights reserved.

Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

About Us

[History & Purpose](#)

[Contact Information](#)


[Terms of Service](#)


[Privacy Statement](#)

[Copyright Information](#)

Hosting By

[Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)