ZDI-CAN-29156: New Vulnerability Report

Moderate **phoerious** published **GHSA-4gr2-cr97-q9fx** on Mar 9

Package

KeePassXC

Affected versions

<=2.7.11

Patched versions

2.7.12

Description

ZDI-CAN-29156: KeePassXC OpenSSL Configuration Uncontrolled Search Path Element Local Privilege Escalation Vulnerability

-- CVSS ----------

7.3: AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

-- ABSTRACT ----------

TrendAI's Zero Day Initiative has identified a vulnerability affecting the following products: KeePassXC - KeePassXC

-- VULNERABILITY DETAILS ----------

- Version Tested: 2.7.11
- Platform Tested: Windows 11 Enterprise 24H2

Analysis

When KeePassXC checks for updates, it uses OpenSSL, and will ingest a configuration file if present at `C:\Tools\vcpkg\packages\openssl_x64-windows\openssl.cnf`. A low-privileged user can create that folder structure and load an arbitrary DLL into KeePassXC when KeePassXC is run by any user on that machine (and KeePassXC checks for updates). Achieving code execution within the process of another user's instance of KeePassXC results in a catastrophic loss of security for the target user's secrets maintained in KeePassXC.

Repro steps

1. Build the x64 Release configuration of the attached solution, `CmdOnDllMain`. A pre-built `CmdOnDllMain.dll` is also included if you prefer.
2. Log on to the target machine as a low-privileged user.
3. At a command prompt, run: `mkdir C:\Tools\vcpkg\packages\openssl_x64-windows`
4. To the `openssl_x64-windows` folder just created, copy `CmdOnDllMain.dll` and `openssl.cnf` (attached).
5. Now, when logging in as *any* user and updating KeePassXC, the malicious DLL `CmdOnDllMain.dll` is loaded into the process. For demonstration, this DLL simply launches and instance of `cmd.exe`, but this demonstrates arbitrary code execution in the `KeePassXC.exe` process of the target user.

```
Date:   2/3/2026 6:55:37.4281104 PM
Thread: 9956
Class:  File System
Operation:  CreateFile
Result: SUCCESS
Path:   C:\Tools\vcpkg\packages\openssl_x64-windows\openssl.cnf
Duration:   0.0000450
Desired Access: Generic Read
Disposition:    Open
Options:    Synchronous IO Non-Alert, Non-Directory File
Attributes: N
ShareMode:  Read, Write
AllocationSize: n/a
OpenResult: Opened

Description:    KeePassXC
Company:    KeePassXC Team
Name:   KeePassXC.exe
Version:    2.7.11
Path:   C:\Program Files\KeePassXC\KeePassXC.exe
Command Line:   "C:\Program Files\KeePassXC\KeePassXC.exe"
PID:    3120
Parent PID: 9220
Session ID: 6
User:   [REDACTED]
Auth ID:    00000000:00efd0f3
Architecture:   64-bit
Virtualized:    False
Integrity:  Medium
Started:    2/3/2026 6:51:43 PM
```

```
Ended:  (Running)
Modules:
KeePassXC.exe   0x7ff6bc350000  0x570000    C:\Program Files\KeePassXC\KeePassXC.exe
KeePassXC Team  2.7.11  11/23/2025 5:59:12 PM
d3d9.dll    0x7ffd7a6e0000  0x1b3000    C:\WINDOWS\system32\d3d9.dll    Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  4/14/1999 8:31:56 PM
keepassxc-autotype-windows.dll  0x7ffd7a8a0000  0x4d7000    C:\Program
Files\KeePassXC\keepassxc-autotype-windows.dll          11/23/2025 5:59:11 PM
qwindows.dll    0x7ffd7ad80000  0xce000 C:\Program
Files\KeePassXC\plugins\platforms\qwindows.dll  The Qt Company Ltd. 5.15.18.0
11/20/2025 7:02:38 AM
harfbuzz.dll    0x7ffd7ae50000  0x126000    C:\Program Files\KeePassXC\harfbuzz.dll
11/20/2025 6:37:25 AM
freetype.dll    0x7ffd7bef0000  0xad000 C:\Program Files\KeePassXC\freetype.dll The
FreeType Project    2.13.3  11/20/2025 6:35:42 AM
libcrypto-3-x64.dll 0x7ffd7bfa0000  0x51a000    C:\Program Files\KeePassXC\libcrypto-
3-x64.dll   The OpenSSL Project, https://www.openssl.org/   3.6.0   11/20/2025
6:33:44 AM
libssl-3-x64.dll    0x7ffd7c4c0000  0xd8000 C:\Program Files\KeePassXC\libssl-3-
x64.dll The OpenSSL Project, https://www.openssl.org/   3.6.0   11/20/2025 6:33:44 AM
botan-3.dll 0x7ffd7c5a0000  0x601000    C:\Program Files\KeePassXC\botan-3.dll
11/20/2025 6:28:59 AM
Qt5Core.dll 0x7ffd7cbb0000  0x50e000    C:\Program Files\KeePassXC\Qt5Core.dll  The
Qt Company Ltd. 5.15.18.0   11/20/2025 6:46:34 AM
Qt5Gui.dll  0x7ffd7d0c0000  0x642000    C:\Program Files\KeePassXC\Qt5Gui.dll   The
Qt Company Ltd. 5.15.18.0   11/20/2025 6:48:14 AM
Qt5Widgets.dll  0x7ffd7d710000  0x54a000    C:\Program Files\KeePassXC\Qt5Widgets.dll
The Qt Company Ltd. 5.15.18.0   11/20/2025 7:00:30 AM
Qt5Network.dll  0x7ffd7dc60000  0x144000    C:\Program Files\KeePassXC\Qt5Network.dll
The Qt Company Ltd. 5.15.18.0   11/20/2025 6:47:20 AM
qwindowsvistastyle.dll  0x7ffd811b0000  0x27000 C:\Program
Files\KeePassXC\plugins\styles\qwindowsvistastyle.dll   The Qt Company Ltd. 5.15.18.0
11/20/2025 7:01:36 AM
brotlicommon.dll    0x7ffd81580000  0x27000 C:\Program
Files\KeePassXC\brotlicommon.dll            11/20/2025 6:35:25 AM
pcre2-16.dll    0x7ffd81a10000  0x8f000 C:\Program Files\KeePassXC\pcre2-16.dll
11/20/2025 6:34:38 AM
libpng16.dll    0x7ffd823b0000  0x35000 C:\Program Files\KeePassXC\libpng16.dll
11/20/2025 6:34:48 AM
Qt5Svg.dll  0x7ffd823f0000  0x52000 C:\Program Files\KeePassXC\Qt5Svg.dll   The Qt
Company Ltd.    5.15.18.0   11/20/2025 7:05:38 AM
brotlidec.dll   0x7ffd82500000  0x11000 C:\Program Files\KeePassXC\brotlidec.dll
11/20/2025 6:35:26 AM
bz2.dll 0x7ffd82870000  0x17000 C:\Program Files\KeePassXC\bz2.dll
11/20/2025 6:35:18 AM
double-conversion.dll   0x7ffd83090000  0x17000 C:\Program Files\KeePassXC\double-
conversion.dll          11/20/2025 6:38:01 AM
minizip.dll 0x7ffd831d0000  0x11000 C:\Program Files\KeePassXC\minizip.dll
11/20/2025 6:29:32 AM
zlib1.dll   0x7ffd863a0000  0x1a000 C:\Program Files\KeePassXC\zlib1.dll        1.3.1
11/20/2025 6:29:28 AM
WinSCard.dll    0x7ffd9e2b0000  0x42000 C:\WINDOWS\SYSTEM32\WinSCard.dll    Microsoft
Corporation 10.0.26100.3323 (WinBuild.160101.0800)  6/9/2002 6:55:48 AM
qsvgicon.dll    0x7ffda1370000  0xe000  C:\Program
Files\KeePassXC\plugins\iconengines\qsvgicon.dll    The Qt Company Ltd. 5.15.18.0
11/20/2025 7:05:45 AM
```

```
MSVCP140_1.dll  0x7ffda15b0000  0x9000  C:\WINDOWS\SYSTEM32\MSVCP140_1.dll  Microsoft
Corporation 14.40.33816.0   5/7/1947 3:49:30 PM
argon2.dll  0x7ffda3350000  0xc000  C:\Program Files\KeePassXC\argon2.dll
11/20/2025 6:18:53 AM
Qt5Concurrent.dll   0x7ffda4310000  0xd000  C:\Program
Files\KeePassXC\Qt5Concurrent.dll   The Qt Company Ltd. 5.15.18.0   11/20/2025
6:46:43 AM
TextShaping.dll 0x7ffda62f0000  0xb3000 C:\WINDOWS\SYSTEM32\TextShaping.dll Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  2/9/2001 11:49:18 PM
qrencode.dll    0x7ffda6760000  0x10000 C:\Program Files\KeePassXC\qrencode.dll
11/20/2025 6:29:22 AM
dataexchange.dll    0x7ffdab9a0000  0x5a000 C:\WINDOWS\system32\dataexchange.dll
Microsoft Corporation   10.0.26100.7309 (WinBuild.160101.0800)  3/12/1944 12:17:35 AM
MSVCP140.dll    0x7ffdafc50000  0x8d000 C:\WINDOWS\SYSTEM32\MSVCP140.dll    Microsoft
Corporation 14.40.33816.0   11/13/1926 4:55:28 AM
SRVCLI.DLL  0x7ffdb0ac0000  0x29000 C:\WINDOWS\SYSTEM32\SRVCLI.DLL  Microsoft
Corporation 10.0.26100.1150 (WinBuild.160101.0800)  8/8/1977 3:00:31 PM
VCRUNTIME140_1.dll  0x7ffdb1d30000  0xc000  C:\WINDOWS\SYSTEM32\VCRUNTIME140_1.dll
Microsoft Corporation   14.40.33816.0   12/28/1977 9:25:30 PM
WINMM.dll   0x7ffdb22a0000  0x35000 C:\WINDOWS\SYSTEM32\WINMM.dll   Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 7/24/1946 9:45:06 PM
NETAPI32.dll    0x7ffdb3290000  0x1a000 C:\WINDOWS\SYSTEM32\NETAPI32.dll    Microsoft
Corporation 10.0.26100.7019 (WinBuild.160101.0800)  6/23/1998 4:31:16 AM
VCRUNTIME140.dll    0x7ffdb3400000  0x1e000 C:\WINDOWS\SYSTEM32\VCRUNTIME140.dll
Microsoft Corporation   14.40.33816.0   8/31/2036 12:37:58 PM
VERSION.dll 0x7ffdb4950000  0xb000  C:\WINDOWS\SYSTEM32\VERSION.dll Microsoft
Corporation 10.0.26100.1150 (WinBuild.160101.0800)  12/30/1905 8:12:48 PM
textinputframework.dll  0x7ffdb50f0000  0x148000
C:\WINDOWS\SYSTEM32\textinputframework.dll  Microsoft Corporation   10.0.26100.7309
(WinBuild.160101.0800)  11/12/1988 9:06:44 AM
MPR.dll 0x7ffdb5360000  0x21000 C:\WINDOWS\SYSTEM32\MPR.dll Microsoft Corporation
10.0.26100.1 (WinBuild.160101.0800) 1/1/1911 12:32:44 PM
npmproxy.dll    0x7ffdb8540000  0x19000 C:\Windows\System32\npmproxy.dll    Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  7/15/1970 10:55:34 AM
dhcpcsvc.dll    0x7ffdb8d60000  0x23000 C:\Windows\System32\dhcpcsvc.dll    Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 7/10/1920 2:19:39 AM
dhcpcsvc6.dll   0x7ffdb8d90000  0x1e000 C:\Windows\System32\dhcpcsvc6.dll   Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 10/28/2032 2:17:22 PM
twinapi.appcore.dll 0x7ffdb9690000  0x244000
C:\WINDOWS\system32\twinapi.appcore.dll Microsoft Corporation   10.0.26100.1
(WinBuild.160101.0800)  2/9/2031 11:11:15 PM
netprofm.dll    0x7ffdba260000  0x70000 C:\Windows\System32\netprofm.dll    Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 9/19/2029 7:03:39 AM
CoreUIComponents.dll    0x7ffdbac00000  0x2e2000
C:\WINDOWS\SYSTEM32\CoreUIComponents.dll    Microsoft Corporation   10.0.26100.7462
11/24/1945 5:39:13 PM
d3d11.dll   0x7ffdbb170000  0x262000    C:\WINDOWS\SYSTEM32\d3d11.dll   Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  7/8/1958 1:25:50 AM
directxdatabasehelper.dll   0x7ffdbb580000  0x63000
C:\WINDOWS\SYSTEM32\directxdatabasehelper.dll   Microsoft Corporation
10.0.26100.7309 (WinBuild.160101.0800)  4/19/1980 5:46:17 PM
qgenericbearer.dll  0x7ffdbb640000  0x10000 C:\Program
Files\KeePassXC\plugins\bearer\qgenericbearer.dll   The Qt Company Ltd. 5.15.18.0
11/20/2025 7:01:21 AM
dwrite.dll  0x7ffdbbdd0000  0x267000    C:\WINDOWS\system32\dwrite.dll  Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 5/2/1963 1:40:19 AM
```

```
CoreMessaging.dll   0x7ffdbd090000  0x127000    C:\WINDOWS\SYSTEM32\CoreMessaging.dll
Microsoft Corporation   10.0.26100.7309 (WinBuild.160101.0800)  12/22/2034 7:34:20 PM
WTSAPI32.dll    0x7ffdbd950000  0x29000 C:\WINDOWS\SYSTEM32\WTSAPI32.dll    Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  2/3/1966 1:00:15 AM
UxTheme.dll 0x7ffdbd9b0000  0xab000 C:\WINDOWS\SYSTEM32\UxTheme.dll Microsoft
Corporation 10.0.26100.7019 (WinBuild.160101.0800)  10/30/2030 10:22:41 AM
dxcore.dll  0x7ffdbda90000  0x44000 C:\WINDOWS\SYSTEM32\dxcore.dll  Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  12/3/2012 9:27:55 AM
dxgi.dll    0x7ffdbdae0000  0x13b000    C:\WINDOWS\SYSTEM32\dxgi.dll    Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  5/13/1961 12:58:12 AM
dwmapi.dll  0x7ffdbdc40000  0x30000 C:\WINDOWS\SYSTEM32\dwmapi.dll  Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 7/25/2013 8:26:18 PM
windows.storage.dll 0x7ffdbe2f0000  0x85e000
C:\WINDOWS\SYSTEM32\windows.storage.dll Microsoft Corporation   10.0.26100.7019
(WinBuild.160101.0800)  9/17/1926 6:51:27 PM
HID.DLL 0x7ffdbeb60000  0xf000  C:\WINDOWS\SYSTEM32\HID.DLL Microsoft Corporation
10.0.26100.1 (WinBuild.160101.0800) 6/30/2005 12:07:12 PM
NETUTILS.DLL    0x7ffdbedd0000  0xd000  C:\WINDOWS\SYSTEM32\NETUTILS.DLL    Microsoft
Corporation 10.0.26100.1882 (WinBuild.160101.0800)  6/9/1997 2:30:00 AM
IPHLPAPI.DLL    0x7ffdbeec0000  0x34000 C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL    Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 4/14/2034 12:47:10 AM
DNSAPI.dll  0x7ffdbef60000  0x12c000    C:\WINDOWS\SYSTEM32\DNSAPI.dll  Microsoft
Corporation 10.0.26100.1591 (WinBuild.160101.0800)  11/4/1976 3:24:08 PM
kernel.appcore.dll  0x7ffdbf460000  0x1b000 C:\WINDOWS\SYSTEM32\kernel.appcore.dll
Microsoft Corporation   10.0.26100.7309 (WinBuild.160101.0800)  5/11/2009 2:46:34 PM
ntmarta.dll 0x7ffdbf580000  0x36000 C:\WINDOWS\SYSTEM32\ntmarta.dll Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 12/6/1947 8:41:08 PM
SspiCli.dll 0x7ffdbf700000  0x49000 C:\WINDOWS\SYSTEM32\SspiCli.dll Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  12/5/2012 1:31:13 PM
USERENV.dll 0x7ffdbfa80000  0x2b000 C:\WINDOWS\SYSTEM32\USERENV.dll Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 9/14/1912 7:09:03 AM
CRYPTBASE.DLL   0x7ffdbfcb0000  0xc000  C:\WINDOWS\SYSTEM32\CRYPTBASE.DLL   Microsoft
Corporation 10.0.26100.7623 (WinBuild.160101.0800)  7/22/2015 6:45:45 PM
WINSTA.dll  0x7ffdc0460000  0x64000 C:\WINDOWS\SYSTEM32\WINSTA.dll  Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  6/17/1999 2:56:00 AM
UMPDC.dll   0x7ffdc0510000  0x14000 C:\WINDOWS\SYSTEM32\UMPDC.dll   Microsoft
Corporation 10.0.26100.7019 (WinBuild.160101.0800)  4/29/2024 3:46:24 PM
powrprof.dll    0x7ffdc0530000  0x5e000 C:\WINDOWS\SYSTEM32\powrprof.dll    Microsoft
Corporation 10.0.26100.4202 (WinBuild.160101.0800)  6/26/1924 1:25:39 PM
profapi.dll 0x7ffdc05d0000  0x29000 C:\WINDOWS\SYSTEM32\profapi.dll Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  6/15/1979 9:32:34 AM
wintypes.dll    0x7ffdc06b0000  0x16a000    C:\WINDOWS\System32\wintypes.dll
Microsoft Corporation   10.0.26100.6725 (WinBuild.160101.0800)  1/21/1975 1:29:23 PM
msvcp_win.dll   0x7ffdc0820000  0xa3000 C:\WINDOWS\System32\msvcp_win.dll   Microsoft
Corporation 10.0.26100.7623 (WinBuild.160101.0800)  6/8/1902 7:37:03 PM
CRYPT32.dll 0x7ffdc08d0000  0x177000    C:\WINDOWS\System32\CRYPT32.dll Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 10/13/1973 11:48:52 PM
win32u.dll  0x7ffdc0a50000  0x27000 C:\WINDOWS\System32\win32u.dll  Microsoft
Corporation 10.0.26100.7623 (WinBuild.160101.0800)  9/5/1987 4:37:14 PM
gdi32full.dll   0x7ffdc0a80000  0x12c000    C:\WINDOWS\System32\gdi32full.dll
Microsoft Corporation   10.0.26100.7309 (WinBuild.160101.0800)  7/23/1987 4:04:26 PM
KERNELBASE.dll  0x7ffdc0bb0000  0x3ef000    C:\WINDOWS\System32\KERNELBASE.dll
Microsoft Corporation   10.0.26100.7309 (WinBuild.160101.0800)  1/16/2007 5:32:31 PM
bcryptPrimitives.dll    0x7ffdc1100000  0xa5000
C:\WINDOWS\System32\bcryptPrimitives.dll    Microsoft Corporation   10.0.26100.7623
(WinBuild.160101.0800)  8/4/1988 6:58:34 AM
```

```
ucrtbase.dll    0x7ffdc11b0000  0x14b000    C:\WINDOWS\System32\ucrtbase.dll
Microsoft Corporation   10.0.26100.7623 (WinBuild.160101.0800)  6/17/2014 11:21:50 AM
GDI32.dll   0x7ffdc1300000  0x2b000 C:\WINDOWS\System32\GDI32.dll   Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  5/2/2028 10:35:33 AM
KERNEL32.DLL    0x7ffdc1440000  0xc9000 C:\WINDOWS\System32\KERNEL32.DLL    Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  11/8/1948 12:22:55 PM
SETUPAPI.dll    0x7ffdc1510000  0x48a000    C:\WINDOWS\System32\SETUPAPI.dll
Microsoft Corporation   10.0.26100.1 (WinBuild.160101.0800) 8/29/1910 7:16:22 AM
RPCRT4.dll  0x7ffdc19a0000  0x118000    C:\WINDOWS\System32\RPCRT4.dll  Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 10/25/1924 10:13:55 PM
shlwapi.dll 0x7ffdc1ac0000  0x66000 C:\WINDOWS\System32\shlwapi.dll Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 7/2/2003 10:38:12 AM
WS2_32.dll  0x7ffdc1b50000  0x74000 C:\WINDOWS\System32\WS2_32.dll  Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 6/18/1957 6:19:34 PM
USER32.dll  0x7ffdc1bd0000  0x1c5000    C:\WINDOWS\System32\USER32.dll  Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 4/7/1906 2:52:26 AM
ADVAPI32.dll    0x7ffdc1da0000  0xb4000 C:\WINDOWS\System32\ADVAPI32.dll    Microsoft
Corporation 10.0.26100.3624 (WinBuild.160101.0800)  9/23/1963 11:57:30 AM
combase.dll 0x7ffdc1e60000  0x386000    C:\WINDOWS\System32\combase.dll Microsoft
Corporation 10.0.26100.6725 (WinBuild.160101.0800)  9/28/1935 6:04:03 AM
MSCTF.dll   0x7ffdc2300000  0x15e000    C:\WINDOWS\System32\MSCTF.dll   Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 9/3/2006 2:01:48 PM
clbcatq.dll 0x7ffdc24c0000  0xb0000 C:\WINDOWS\System32\clbcatq.dll Microsoft
Corporation 2001.12.10941.16384 (WinBuild.160101.0800)  11/21/1965 10:14:29 AM
sechost.dll 0x7ffdc2580000  0xa6000 C:\WINDOWS\System32\sechost.dll Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 6/12/1940 6:07:49 PM
OLEAUT32.dll    0x7ffdc2630000  0xd6000 C:\WINDOWS\System32\OLEAUT32.dll    Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  8/25/1907 9:16:08 AM
IMM32.DLL   0x7ffdc2920000  0x31000 C:\WINDOWS\System32\IMM32.DLL   Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  9/22/1968 7:11:56 PM
SHELL32.dll 0x7ffdc2a50000  0x753000    C:\WINDOWS\System32\SHELL32.dll Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  5/9/1910 7:08:17 AM
ole32.dll   0x7ffdc31c0000  0x197000    C:\WINDOWS\System32\ole32.dll   Microsoft
Corporation 10.0.26100.6725 (WinBuild.160101.0800)  8/6/1952 12:20:45 PM
shcore.dll  0x7ffdc3360000  0xf5000 C:\WINDOWS\System32\shcore.dll  Microsoft
Corporation 10.0.26100.1 (WinBuild.160101.0800) 2/13/2034 12:05:08 AM
NSI.dll 0x7ffdc3460000  0xa000  C:\WINDOWS\System32\NSI.dll Microsoft Corporation
10.0.26100.7623 (WinBuild.160101.0800)  1/14/1910 8:30:58 AM
msvcrt.dll  0x7ffdc3470000  0xa9000 C:\WINDOWS\System32\msvcrt.dll  Microsoft
Corporation 7.0.26100.7623 (WinBuild.160101.0800)   5/7/1966 11:05:07 PM
ntdll.dll   0x7ffdc3560000  0x267000    C:\WINDOWS\SYSTEM32\ntdll.dll   Microsoft
Corporation 10.0.26100.7309 (WinBuild.160101.0800)  8/10/2018 12:48:14 PM


0   FLTMGR.SYS  FltpPerformPreCallbacksWorker + 0x58f   0xfffff8074ccabaaf
C:\WINDOWS\System32\drivers\FLTMGR.SYS
1   FLTMGR.SYS  FltpPassThroughInternal + 0xc0  0xfffff8074ccab1a0
C:\WINDOWS\System32\drivers\FLTMGR.SYS
2   FLTMGR.SYS  FltpCreate + 0x6f0  0xfffff8074cd17c40
C:\WINDOWS\System32\drivers\FLTMGR.SYS
3   ntoskrnl.exe    IopfCallDriver + 0x5b   0xfffff807bb3913db
C:\WINDOWS\system32\ntoskrnl.exe
4   ntoskrnl.exe    IofCallDriver + 0x13    0xfffff807bb391353
C:\WINDOWS\system32\ntoskrnl.exe
5   ntoskrnl.exe    IopParseDevice + 0x73b  0xfffff807bb89690b
C:\WINDOWS\system32\ntoskrnl.exe
```

```
6   ntoskrnl.exe    ObpLookupObjectName + 0xe4a 0xfffff807bb8949aa
C:\WINDOWS\system32\ntoskrnl.exe
7   ntoskrnl.exe    ObOpenObjectByNameEx + 0x223    0xfffff807bb8926b3
C:\WINDOWS\system32\ntoskrnl.exe
8   ntoskrnl.exe    IopCreateFile + 0x1038  0xfffff807bb96d728
C:\WINDOWS\system32\ntoskrnl.exe
9   ntoskrnl.exe    NtCreateFile + 0x79 0xfffff807bb96c6d9
C:\WINDOWS\system32\ntoskrnl.exe
10  ntoskrnl.exe    KiSystemServiceCopyEnd + 0x25   0xfffff807bb6b5755
C:\WINDOWS\system32\ntoskrnl.exe
11  ntdll.dll   NtCreateFile + 0x14 0x7ffdc36c2664  C:\WINDOWS\SYSTEM32\ntdll.dll
12  KERNELBASE.dll  CreateFileInternal + 0x373  0x7ffdc0bf5fd7
C:\WINDOWS\System32\KERNELBASE.dll
13  KERNELBASE.dll  CreateFileW + 0x97  0x7ffdc0bf78c7
C:\WINDOWS\System32\KERNELBASE.dll
14  ucrtbase.dll    wsopen_nolock + 0xf4    0x7ffdc11e9c3c
C:\WINDOWS\System32\ucrtbase.dll
15  ucrtbase.dll    common_sopen_dispatch<wchar_t> + 0x65   0x7ffdc11e9ac9
C:\WINDOWS\System32\ucrtbase.dll
16  ucrtbase.dll    common_openfile<wchar_t> + 0x5e 0x7ffdc11e96f2
C:\WINDOWS\System32\ucrtbase.dll
17  ucrtbase.dll    common_fsopen<wchar_t> + 0x6c   0x7ffdc11ead44
C:\WINDOWS\System32\ucrtbase.dll
18  libcrypto-3-x64.dll OPENSSL_DIR_read + 0x53a    0x7ffd7c1cf84a  C:\Program
Files\KeePassXC\libcrypto-3-x64.dll
19  libcrypto-3-x64.dll BIO_new_file + 0x1d 0x7ffd7c0dd7ed  C:\Program
Files\KeePassXC\libcrypto-3-x64.dll
20  libcrypto-3-x64.dll EVP_CIPHER_get_nid + 0x820  0x7ffd7c11b0b0  C:\Program
Files\KeePassXC\libcrypto-3-x64.dll
21  libcrypto-3-x64.dll CONF_modules_load_file_ex + 0x14a   0x7ffd7c11e1ba
C:\Program Files\KeePassXC\libcrypto-3-x64.dll
22  libcrypto-3-x64.dll OPENSSL_config + 0xbf   0x7ffd7c11f03f  C:\Program
Files\KeePassXC\libcrypto-3-x64.dll
23  libcrypto-3-x64.dll OPENSSL_init_crypto + 0x674 0x7ffd7c1cca04  C:\Program
Files\KeePassXC\libcrypto-3-x64.dll
24  libcrypto-3-x64.dll CRYPTO_THREAD_run_once + 0x55   0x7ffd7c1dcb45  C:\Program
Files\KeePassXC\libcrypto-3-x64.dll
25  libcrypto-3-x64.dll OPENSSL_init_crypto + 0x346 0x7ffd7c1cc6d6  C:\Program
Files\KeePassXC\libcrypto-3-x64.dll
26  libssl-3-x64.dll    OPENSSL_init_ssl + 0x77 0x7ffd7c4d3d97  C:\Program
Files\KeePassXC\libssl-3-x64.dll
27  Qt5Network.dll  QSslEllipticCurve::shortName + 0x2e2b   0x7ffd7dd1c87b
C:\Program Files\KeePassXC\Qt5Network.dll
28  Qt5Network.dll  QSslEllipticCurve::shortName + 0x2d89   0x7ffd7dd1c7d9
C:\Program Files\KeePassXC\Qt5Network.dll
29  Qt5Network.dll  QSslSocket::defaultCiphers + 0xa2   0x7ffd7dd0e0a2  C:\Program
Files\KeePassXC\Qt5Network.dll
30  Qt5Network.dll  QSslConfiguration::defaultConfiguration + 0xe   0x7ffd7dd078de
C:\Program Files\KeePassXC\Qt5Network.dll
31  Qt5Network.dll  QNetworkRequest::sslConfiguration + 0x2c    0x7ffd7dc76fec
C:\Program Files\KeePassXC\Qt5Network.dll
32  Qt5Network.dll  QTcpServer::proxy + 0x13219 0x7ffd7dcb77a9  C:\Program
Files\KeePassXC\Qt5Network.dll
33  Qt5Network.dll  QNetworkAccessManager::createRequest + 0x7c0    0x7ffd7dc66a50
C:\Program Files\KeePassXC\Qt5Network.dll
34  Qt5Network.dll  QNetworkAccessManager::get + 0x1b   0x7ffd7dc673db  C:\Program
```

```
Files\KeePassXC\Qt5Network.dll
35  KeePassXC.exe   AutoTypeExecutor::~AutoTypeExecutor + 0x95bde   0x7ff6bc3fcb1e
C:\Program Files\KeePassXC\KeePassXC.exe
36  KeePassXC.exe   AutoTypeExecutor::~AutoTypeExecutor + 0x162f8   0x7ff6bc37d238
C:\Program Files\KeePassXC\KeePassXC.exe
37  Qt5Core.dll QObject::qt_static_metacall + 0x1270    0x7ffd7cd85780  C:\Program
Files\KeePassXC\Qt5Core.dll
38  Qt5Widgets.dll  QAction::activate + 0x130   0x7ffd7d715d50  C:\Program
Files\KeePassXC\Qt5Widgets.dll
39  Qt5Widgets.dll  QMenu::actionGeometry + 0x4f6   0x7ffd7d86a3e6  C:\Program
Files\KeePassXC\Qt5Widgets.dll
40  Qt5Widgets.dll  QMenu::actionGeometry + 0x2eb   0x7ffd7d86a1db  C:\Program
Files\KeePassXC\Qt5Widgets.dll
41  Qt5Widgets.dll  QMenu::mouseReleaseEvent + 0xb1 0x7ffd7d86f7b1  C:\Program
Files\KeePassXC\Qt5Widgets.dll
42  Qt5Widgets.dll  QWidget::event + 0x12e  0x7ffd7d74716e  C:\Program
Files\KeePassXC\Qt5Widgets.dll
43  Qt5Widgets.dll  QMenu::event + 0xe6 0x7ffd7d86b946  C:\Program
Files\KeePassXC\Qt5Widgets.dll
44  Qt5Widgets.dll  QApplicationPrivate::notify_helper + 0x10d  0x7ffd7d7248bd
C:\Program Files\KeePassXC\Qt5Widgets.dll
45  Qt5Widgets.dll  QApplication::notify + 0x736    0x7ffd7d722896  C:\Program
Files\KeePassXC\Qt5Widgets.dll
46  Qt5Core.dll QCoreApplication::notifyInternal2 + 0xbb    0x7ffd7cd6751b
C:\Program Files\KeePassXC\Qt5Core.dll
47  Qt5Widgets.dll  QApplicationPrivate::sendMouseEvent + 0x3e6 0x7ffd7d725c16
C:\Program Files\KeePassXC\Qt5Widgets.dll
48  Qt5Widgets.dll  QSizePolicy::QSizePolicy + 0x27b9   0x7ffd7d76f6f9  C:\Program
Files\KeePassXC\Qt5Widgets.dll
49  Qt5Widgets.dll  QSizePolicy::QSizePolicy + 0xbe1    0x7ffd7d76db21  C:\Program
Files\KeePassXC\Qt5Widgets.dll
50  Qt5Widgets.dll  QApplicationPrivate::notify_helper + 0x10d  0x7ffd7d7248bd
C:\Program Files\KeePassXC\Qt5Widgets.dll
51  Qt5Widgets.dll  QApplication::notify + 0x1827   0x7ffd7d723987  C:\Program
Files\KeePassXC\Qt5Widgets.dll
52  Qt5Core.dll QCoreApplication::notifyInternal2 + 0xbb    0x7ffd7cd6751b
C:\Program Files\KeePassXC\Qt5Core.dll
53  Qt5Gui.dll  QGuiApplicationPrivate::processMouseEvent + 0x92b   0x7ffd7d10a06b
C:\Program Files\KeePassXC\Qt5Gui.dll
54  Qt5Gui.dll  QWindowSystemInterface::sendWindowSystemEvents + 0x8b
0x7ffd7d0f06db  C:\Program Files\KeePassXC\Qt5Gui.dll
55  Qt5Core.dll QEventDispatcherWin32::processEvents + 0x8b 0x7ffd7cdae3cb
C:\Program Files\KeePassXC\Qt5Core.dll
56  qwindows.dll    qt_plugin_query_metadata + 0x1e49   0x7ffd7ade5769  C:\Program
Files\KeePassXC\plugins\platforms\qwindows.dll
57  Qt5Core.dll QEventLoop::exec + 0x1c0    0x7ffd7cd63ab0  C:\Program
Files\KeePassXC\Qt5Core.dll
58  Qt5Core.dll QCoreApplication::exec + 0x154  0x7ffd7cd66494  C:\Program
Files\KeePassXC\Qt5Core.dll
59  KeePassXC.exe   KeePassXC.exe + 0xfe89  0x7ff6bc35fe89  C:\Program
Files\KeePassXC\KeePassXC.exe
60  KeePassXC.exe   AutoTypeMode::exec + 0x560e6    0x7ff6bc565ca6  C:\Program
Files\KeePassXC\KeePassXC.exe
61  KeePassXC.exe   AutoTypeMode::exec + 0x54df2    0x7ff6bc5649b2  C:\Program
Files\KeePassXC\KeePassXC.exe
62  KERNEL32.DLL    BaseThreadInitThunk + 0x17  0x7ffdc146e8d7
```

```
C:\WINDOWS\System32\KERNEL32.DLL
63  ntdll.dll   RtlUserThreadStart + 0x2c   0x7ffdc35ec53c
C:\WINDOWS\SYSTEM32\ntdll.dll
```

-- CREDIT ----------
This vulnerability was discovered by:
Xavier DANEST working with TrendAI Zero Day Initiative

-- FURTHER DETAILS ----------

Supporting files:
https://trendmicro-my.sharepoint.com/:u:/p/mai_mostafa/IQDH4VsvK622Rosy4CL_3wO-AXtZnvIX9o7j4Czfz_rTqKs?e=jQHyQl

If supporting files were contained with this report they are provided within a password protected ZIP file. The password is the ZDI candidate number in the form: ZDI-CAN-XXXX where XXXX is the ID number.

Please confirm receipt of this report. We expect all vendors to remediate ZDI vulnerabilities within 120 days of the reported date. If you are ready to release a patch at any point leading up to the deadline, please coordinate with us so that we may release our advisory detailing the issue. If the 120-day deadline is reached and no patch has been made available we will release a limited public advisory with our own mitigations, so that the public can protect themselves in the absence of a patch. Please keep us updated regarding the status of this issue and feel free to contact us at any time:

Zero Day Initiative
zdi-disclosures@trendmicro.com

The PGP key used for all ZDI vendor communications is available from:

http://www.zerodayinitiative.com/documents/disclosures-pgp-key.asc

-- INFORMATION ABOUT THE ZDI ----------
Established by TippingPoint and acquired by Trend Micro, the Zero Day Initiative (ZDI) neither re-sells vulnerability details nor exploit code. Instead, upon notifying the affected product vendor, the ZDI provides its Trend Micro TippingPoint customers with zero day protection through its intrusion prevention technology. Explicit details regarding the specifics of the vulnerability are not exposed to any parties until an official vendor patch is publicly available.

Please contact us for further details or refer to:

http://www.zerodayinitiative.com

-- DISCLOSURE POLICY ----------

Our vulnerability disclosure policy is available online at:

http://www.zerodayinitiative.com/advisories/disclosure_policy/

Severity

Moderate

CVE ID

No known CVE

Weaknesses

▶ CWE-427

Credits

zdi-disclosures Reporter