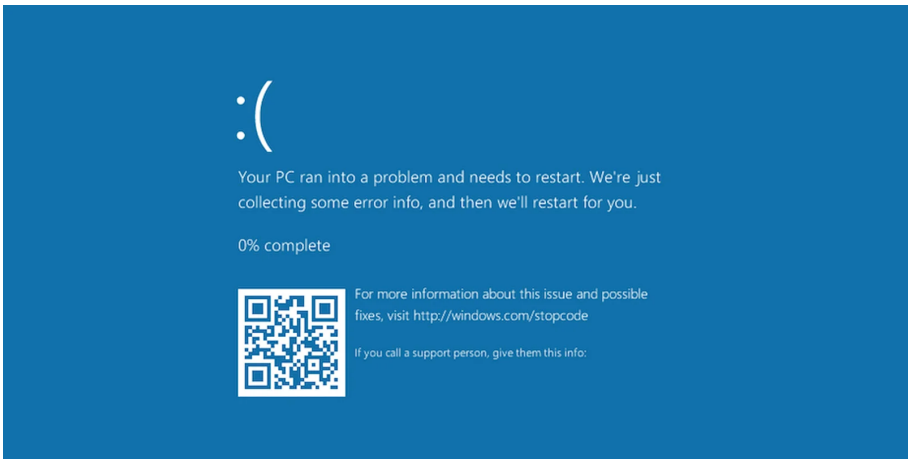
Windows 10 bug crashes your PC when you access this location

By Lawrence Abrams

January 17, 2021 03:21 PM 8



A bug in Windows 10 causes the operating system to crash with a Blue Screen of Death simply by opening a certain path in a browser's address bar or using other Windows commands.

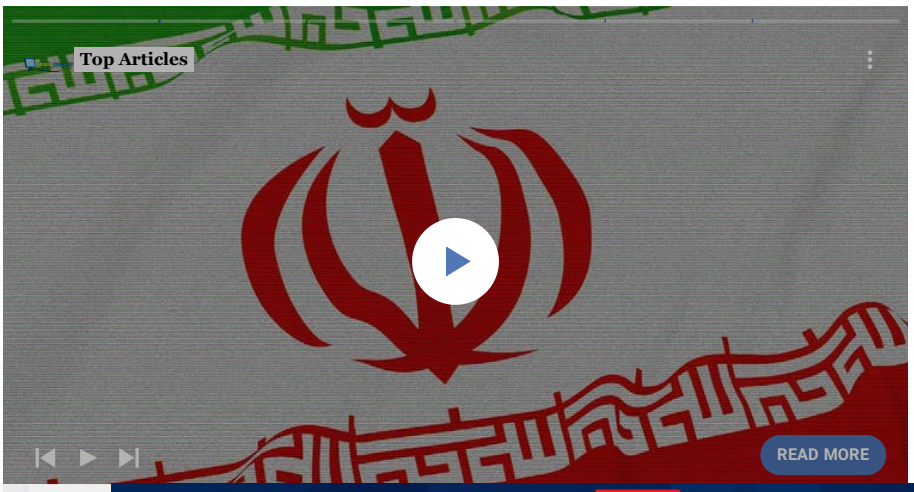
Last week, BleepingComputer learned of two bugs disclosed on Twitter by a Windows security researcher that can be abused by attackers in various attacks.

The first bug allows an unprivileged user or program to enter a single command that causes an NTFS volume to become marked as corrupted. While chkdsk resolved this issue in many tests, one of our tests showed that the command caused corruption on a hard drive that prevented Windows from starting.

POPULAR STORIES

Microsoft: May Windows updates cause AD authentication failures

FBI, CISA, and NSA warn of hackers increasingly targeting MSPs



Opening this path causes a BSOD

A Windows 10 bug first discovered by security researcher Walied Assar, and later publicly disclosed by security researcher Jonas Lykkegaard, causes Windows 10 to crash and display a BSOD when a special path is entered into the Chrome address bar.

When developers want to interact with Windows devices directly, they can pass a Win32 device namespace path as an argument to various Windows programming functions. For example, this allows an application to interact directly with a physical disk without going through the file system.

Lykkegaard told BleepingComputer that he discovered the following Win32 device namespace path for the 'console multiplexer driver' that he believes is used for 'kernel / usermode ipc.' When opening the path in various ways, even from low-privileged users, it would cause Windows 10 to crash.

```
\\.\globalroot\device\condrv\kernelconnect
```

When connecting to this device, developers are expected to pass along the 'attach' extended attribute to communicate with the device properly.

```
__int64 __fastcall CdCreateKernelConnection(PIRP Irp)
{
  char v1; // r12
  char *v3; // r14
  int v4; // esi
  struct _IO_STACK_LOCATION *v5; // r13
  __int64 v6; // rax
  _LIST_ENTRY *v7; // rdi
  char *v8; // rbp
  struct _IO_STACK_LOCATION *v9; // rax
  _LIST_ENTRY *v10; // r15
  _LIST_ENTRY *v11; // rcx
  struct _IRP::$::$2AD798E65616C4F7304824DBFA27E419::$665C8370128C04AB892B069E6FB086E8 *v12; // rax
  char *v13; // rax
  __int64 v14; // rbx
  _LIST_ENTRY *v16; // [rsp+60h] [rbp+8h] BYREF
  PVOID P; // [rsp+70h] [rbp+18h] BYREF

  v1 = 0;
  v3 = 0i64;
  v16 = 0i64;
  P = 0i64;
  if ( Irp->RequestorMode )
    return (unsigned int)-1073741790;
  v5 = Irp->Tail.Overlay.CurrentStackLocation;
  v6 = CdpFindEaBufferItem(Irp->AssociatedIrp.MasterIrp, "attach");
  if ( !v6 || *(_WORD *)(v6 + 6) != 8 )
    return (unsigned int)-1073741811;
  v4 = CdpGetProcessServerFromConnection(&P, Irp, *(_QWORD *)(*(unsigned __int8 *)(v6 + 5) + v6 + 9));
  if ( v4 < 0 )
  {
    v7 = (_LIST_ENTRY *)P;
    goto LABEL_31;
  }
  KeEnterCriticalRegion();
  v7 = (_LIST_ENTRY *)P;
```

CDCreateKernlConnection showing the 'attach' extended attribute

Lykkegaard discovered if you try to connect to the path without passing the attribute due to improper error checking, it will cause an exception that causes a Blue Screen of Death (BSOD) crash in Windows 10.

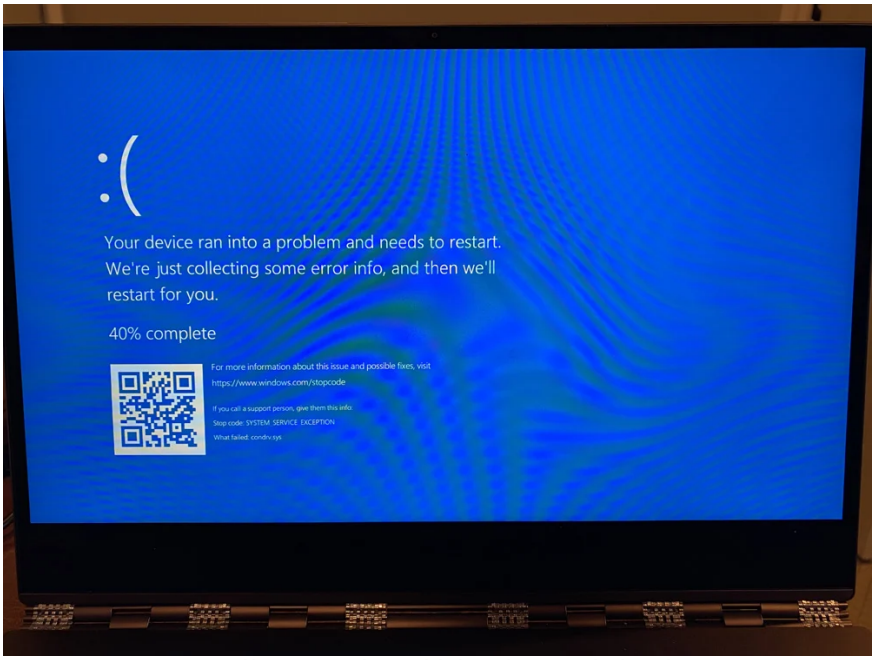
Even worse, low privileged Windows users can attempt to connect to the device using this path, making it easy for any program executed on a computer to crash Windows 10.

In our tests, we have confirmed this bug to be present on Windows 10 version 1709 and later. BleepingComputer was unable to test it in earlier versions.

BleepingComputer reached out to Microsoft last week to learn if they knew of the bug already and if they

While it has not been determined if this bug could be exploited for remote code execution or elevation privilege, in its current form, it can be used as a denial of service attack on a computer.

Lykkegaard shared with BleepingComputer a Windows URL file (.url) with a setting pointing to \\.\globalroot\device\condrv\kernelconnect. When the file is downloaded, Windows 10 would try to render the URL file's icon from the problematic path and automatically crash Windows 10.



BSOD caused by accessing the \\.\globalroot\device\condrv\kernelconnect

BleepingComputer has since found numerous other ways to exploit this bug, including methods to cause BSODs automatically on Windows login.

In a real-life scenario, this bug could be abused by threat actors who have access to a network and want to cover their trail during an attack.

If they have admin credentials, they could remotely execute a command that accesses this path on all of the Windows 10 devices on a network to cause them to crash. The havoc caused on the network could delay investigations or prevent administrative controls from detecting an attack on a particular computer.

In 2017, a similar attack scenario was used by threat actors during a bank heist on the Far Eastern International Bank (FEIB) in Taiwan. In that attack, the threat actors deployed the Hermes ransomware on the network to delay investigations into the attack.

Update 2/8/21: Added Walied Assar as the original discoverer of this vulnerability.

Related Articles:

Microsoft fixes Bluetooth issue causing Windows blue screens

Microsoft May 2022 Patch Tuesday fixes 3 zero-days, 75 flaws

Google Docs crashes on seeing "And. And. And. And. And."

Microsoft PowerShell lets you track Windows Registry changes

Fake Windows 10 updates infect you with Magniber ransomware

LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

PREVIOUS ARTICLE NEXT ARTICLE

Comments

BrechtMo - 1 year ago

I successfully crashed a W10 1909.
Windows event log only recorded generic bugcheck (1001) and kernel-power (42) events.
Bluescreenview identified condrv.sys as the cause of the crash in the .dmp file so you could check on that to verify that this issue was (most likely) the cause of a crash.

d-reaper - 1 year ago

I just tried it. Haha! This is neat! Another reason why I'm glad I don't use Windows as my daily driver anymore. I've never used 10 as my daily driver, and I'm no where near close to consider doing so. KDE Neon has saved my sanity that Windows 10 (And all of its other issues), otherwise would have taken from me.

Larita - 1 year ago

Hello!

Thanks for this info. Do We have a solution to prevent this?

Ethanmiller123 - 1 year ago

There was a bug where I just had to open a blank file as a video file in Media player on a version of Windows 10 and it crashed. It's probably patched now.

bob3160 - 1 year ago

So does this also address the following bug? https://youtu.be/JjgcyqiT33M If not, has it already been patched or, is a patch still in the works?

Lawrence Abrams - 1 year ago

That video is about this bug. Still not patched

DRSION - 1 year ago

Good afternoon, Is there an official statement, or a record by Microsoft where you can follow up on this news? or they can indicate if there is an associated CVE record.

Thank you very much.

and Firefox "Your file couldn't be accessed It may have been moved, edited or deleted.
ERR_FILE_NOT_FOUND"

Post a Comment

Community Rules

You need to login in order to post a comment

Login

Not a member yet? Register Now

You may also like: